Machine Translated by Google

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

En plan for digital identitet

Finansielle institutioners rolle i opbygningen af digital identitet

Et brancheprojekt for den finansielle sektor | Udarbejdet i samarbejde med Deloitte

En del af serien Fremtiden for finansielle tjenester • August 2016

Machine Translated by Google

Forord

I overensstemmelse med World Economic Forums mission om at anvende en multistakeholder-tilgang til at håndtere problemstillinger med global indvirkning, involverede udarbejdelsen af denne rapport omfattende opsøgende arbejde og dialog med finansielle servicesektoren, innovationsmiljøet, teknologimiljøet, den akademiske verden og den offentlige sektor. Dialogen omfattede adskillige interviews og interaktive sessioner for at diskutere indsigter og muligheder for fælles handling.

Vi takker industrien og fageksperterne, der har bidraget med deres unikke indsigter til denne rapport, oprigtigt. Især medlemmerne af projektets styregruppe og arbejdsgruppe, som præsenteres på de følgende sider, spillede en uvurderlig rolle som eksperter og patientmentorer.

Vi er også meget taknemmelige for den generøse indsats og støtte til Deloitte Consulting LLP i USA, en enhed inden for Deloitte1-netværket, i deres egenskab af officiel rådgiver for professionelle tjenester til World Economic Forum i forbindelse med dette projekt.

Kontakte

For feedback eller spørgsmål, kontakt venligst:

R. Jesse McWaters, hovedforfatter
jesse.mcwaters@weforum.org +1
(212) 703ÿ6633

1 Deloitte henviser til en eller flere af Deloitte Touche Tohmatsu Limited, et britisk privat selskab med begrænset ansvar ("DTTL"), dets netværk af medlemsfirmaer og deres relaterede enheder. DTTL og hvert af dets medlemsfirmaer er juridisk separate og uafhængige enheder. DTTL (også kaldet "Deloitte Global") leverer ikke tjenester til klienter. Se www.deloitte.com/about for en detaljeret beskrivelse af DTTL og dets medlemsfirmaer. Se www.deloitte.com/us/about for en detaljeret beskrivelse af den juridiske struktur af Deloitte LLP og dets datterselskaber. Visse tjenester er muligvis ikke tilgængelige for attesterende klienter i henhold til reglerne og bestemmelserne for offentlig regnskabsføring.

Denne publikation indeholder kun generelle oplysninger, og Deloitte yder ikke ved hjælp af denne publikation regnskabsmæssig, forretningsmæssig, finansiel, investeringsmæssig, juridisk, skattemæssig eller anden professionel rådgivning eller tjenesteydelse. Denne publikation erstatter ikke sådan professionel rådgivning eller tjenesteydelse, og den bør heller ikke bruges som grundlag for nogen beslutning eller handling, der kan påvirke din virksomhed. Før du træffer nogen beslutning eller foretager nogen handling, der kan påvirke din virksomhed, bør du konsultere en kvalificeret professionel rådgiver. Deloitte er ikke ansvarlig for tab, der påføres personer, der stoler på denne publikation.

Machine Translated by Google

Taksigelser

Machine Translated by Google

Taksigelser

Medlemmer af styringskomitéen

Følgende ledende medarbejdere fra globale finansielle institutioner har ydet vejledning, tilsyn og tankelederskab til "Disruptive" Projektet "Innovation i finansielle tjenester" som styregruppe:

Bob Contri

Næstformand,
Deloitte & Touche LLP

David Craig

Direktør, Risiko og Finans,
Thomson Reuters

John Flint

Administrerende direktør, Retail Banking og Formueforvaltning, *HSBC*

Kim Hammond

Driftsdirektør,
Deutsche Bank

Jason Harris

Administrerende direktør, International Ejendom og skader, *XL Group*

Michael Harte

Teknologichef og chef Driftschef, *Barclays*

Axel Lehmann

Driftsdirektør,
UBS

Anju Patwardhan

Innovationschef,
Standard Chartered Bank

David Puth

Administrerende direktør,
CLS-gruppen

William Sheedy

Global leder, virksomhedsstrategi, fusioner og opkøb, Offentlige relationer, *Visa*

Dietter Wemmer

Finansdirektør,
Allianz

Machine Translated by Google

Projektteamet vil også gerne takke følgende ledere fra globale finansielle institutioner, som hjalp med at definere projektets rammer og udforme strategiske analyser som arbejdsgruppe:

Tom Brown

Partner,
Paul Hastings

Lena Mass-Cresnik, ph.d.

Innovationschef, Strategisk Produkt
Ledelse, *BlackRock*

Christof Edel

Global chef for handelsstrategi og forretning
Udvikling, *Thomson Reuters*

Rob Galaski *(projektrådgiver)*

Chef for finansielle tjenester,
Deloitte

Dorothy Hillenius

Direktør for virksomhedsstrategi,
ING

Marc Lien

Direktør for Innovation og Digitalisering
Udvikling, *Lloyds Banking Group*

Matthew Levin

EVP og chef for global strategi,
Aon

Victor Matarranz

Strategidirektør og stabschef for administrerende direktør,
Santander

Neil Mumm

VP for virksomhedsstrategi,
Visum

Max Neukirchen

Koncernchef for strategi,
JP Morgan Chase

Christine O'Connell

Global chef for strategi og forretning
Udvikling, *Thomson Reuters*

Robert Palatnick

Administrerende direktør og chefteknologi
Arkitekt, *DTCC*

Kosta Peric

Vicedirektør for finansielle tjenester for
Fattig, *Bill og Melinda Gates Foundation*

Justin Pinkham

Senior Vice President og koncernchef, Betalingsinnovation,
MasterCard

Bob Reany

Senior vicedirektør og koncernchef, Identity Solutions
MasterCard

Peter Rutland

Senior administrerende direktør,
CVC Capital Partners

Nicolas de Skowronski

Stabschef,
Bank Julius Bær

Huw Van Steenis

Administrerende direktør og økonomichef
Serviceforskning, *Morgan Stanley*

Colin Teichholtz

Partner og medchef for obligationshandel,
Pine River Capital

Fabien Vandenreydt

Chef for Markedsstyring, Innotribe & the
SWIFT-instituttet, *SWIFT*

Machine Translated by Google

Derudover udtrykker projektgruppen sin taknemmelighed til følgende fageksperter, der har bidraget med deres værdifulde perspektiver.

gennem interviews og workshops (i alfabetisk rækkefølge):

Mukul Ahuja	Deloitte Canada
Christoph Albers	SWIFT
Alex Batlin	UBS
Erik Benz	Kreditter
Peter Berg	Visum
Vikram Bhat	Deloitte & Touche LLP
David Birch	Konsulter Hyperion
Francis Bouchard	Hamilton Place Strategier
Andre Boysen	Sikkerhedsnøgle
David Brygger	Digital katapult
Ben Brophy	ENTIQ
Tom Brown	Paul Hastings
Preston Byrne	Eris Industries
Claire Calmejane	Lloyds Banking Group
Alicia Carmona	Identitet 2020
Nicolas Cary	Blockchain
Shawn Chance	Nymi
Emily Clayton	Bank of England
John Klippinger	MIT Media Lab
Jeff Coleman	Ledger Labs
Wayne Crombie	Citigroup
Malcolm Crompton	Informationsintegritetsløsninger
Stephen Cross	Aon
Mark Davies	Avox Ltd.
Howard Davis	RBS
Nicolas de Skowronski	Julius Bær
Rachel Dixon	Australiens kontor for digital transformation
Ivan Djordjeviÿ	Deloitte UK
Justin Dombrowski	Historiocity Tech
Jon Duffy	TradeMe
Carlo Duprel	Deloitte Skat & Rådgivning, Luxembourg
André Durand	Ping-identitet
John Edge	Digital lagret værdiforening
Anna Ewing	Nasdaq
Daniel Feichtinger	Digitale aktiver
Chris Ferguson	Det britiske kabinetskontor
Jerry Fishenden	VoeTek
Marissa Flowerday	TradeMe
Conan French	IIF
Emilio Garcia	Santander
Joe Guastella	Deloitte Consulting LLP
Alka Gupta	Globalt ID
Aran Hamilton	DIACC
Jonathan Hardinges	Thomson Reuters
Adrienne Harris	Det Nationale Økonomiske Råd, Det Hvide Hus
Jonathan Hayes	Julius Bær
Dorothy Hillenius	ING
Bill Hodash	DTCC
Rainer Hörbe	Kantara-initiativet
Chuck Hounsell	TD Canada
Arne Vidar Huag	Signicat
Afsar Hussain	GSMA
Marta Ienco	GSMA
Raj Iyer	BNY Mellon
Natasha Jackson	GSMA
Charlotte Jacoby	Digitaliseringsstyrelsen, Finansministeriet, Danmark
Hyder Jaffrey	UBS
Andrew Johnston	TELUS
Tanis Jorge	Trulioo
Sean Kevelighan	Zürich Forsikringsgruppe
Alim Khalique	Bank of America Merrill Lynch
Hwan Kim	Deloitte Canada
Dan Kimerling	Standard Treasury
Philipp Kroemer	Commerzbank AG
Jaap Kuipers	Kantara-initiativet
Jo Lambert	Paypal
Ian Lee	Citi
Chris Locke	Caribou Digital
Joseph Lubin	Konsensus
Adam Ludwin	Kæde
Christian Lundkvist	Konsensus

Machine Translated by Google

Derudover udtrykker projektgruppen sin taknemmelighed til følgende fageksperter, der har bidraget med deres værdifulde perspektiver.

gennem interviews og workshops (i alfabetisk rækkefølge):

Joanna Marathakis	Deloitte Transaktioner og Forretningsanalyse LLP
Stephen Marshall	Deloitte UK
Simon Martin	LeapFrog Investments
Todd McDonald	R3CEV
Morgan McKenney	Citigroup
Adel Melek	Deloitte Canada
Pat Meredith	Canadisk betalingstaskforce
Paul Morgenthaler	Commerzbank
Renny Narváez	BNY Mellon
Eddie Neistat	AlixPartners
Nina Nieuwoudt	Mastercard
Pascal Nizri	Tjek
Robert Palatnick	DTCC
Cheryl Parker Rose	CFPB
Justin Pinkham	MasterCard
Rick Porter	Deloitte & Touche LLP
Reinhard Posch	Østrigs føderale regering
Dan Quan	CFPB
Rhomaios Ram	Deutsche Bank
Kai Rannenberg	Goethe-universitetet
Bob Reany	Mastercard
David Richards	DIACC
Pierre Roberge	Konsulent for digital og betalingsinnovation
Andre Romanovskij	Deloitte Canada
Andrew Rudd	AssureUK
Peter Rutland	CVC Capital Partners
Wiebe Ruttenberg	Den Europæiske Centralbank
Joel Sacmar	Daon
Jean-Louis Schiltz	Schiltz & Schiltz
Charles Schwarz	Barclays
Rocky Scopelliti	Telstra
Amy Scott	Identitet2020
John Scott	2Keys Sikkerhedsløsninger
Anton Semenov	Commerzbank
Beth Shah	Digitale aktiver
Rajesh Shenoy	Citi
Nick Smaling	Deloitte Holland
Stan Stalnaker	HubID
Matthew Stauffer	Clarient Entity Hub
Gavin Steele	Lloyd's i London
Ashley Stevenson	ForgeRock
Matt Stroud	Digital katapult
Paul Szurek	Blockchain
Pavlo Tanasyuk	BlokVerificer
Marc Taverner	BitFury
Simon Taylor	Barclays
Adizah Tejani	Niveau 39
Kenneth Tessem	Finansiell ID-Teknik BID AB
Don Thibeau	Åben identitetsudveksling (OIX)
Michael Turner	PERC
Keith Uber	Globalt tegn
Erik Van der Kleij	Niveau 39
Huw van Steenis	Morgan Stanley
Aneesh Varma	Aire.io
Ivan Vatchkov	Algebris Investments
Roy Vella	Vella Ventures Ltd.
Helene Vigue	GSMA
Franziska von Arnim	Deutsche Bank
Patrick Walker	PERC
Colin Wallis	Kantara-initiativet
Peter Watkins	Britisk Columbias regering
Derek White	Barclays
Conor White	Daon
Greg Williamson	MasterCard
Gregory Williamson	MasterCard
Stephan Wolf	GLEIF
Kevin Young	Deloitte Canada
Fei Zhang	Allianz
Tom Zschach	CLS Bank

Machine Translated by Google

Taksigelser

Projektteam og yderligere tak

Projektteam

Projektteamet “Disruptiv innovation i finansielle tjenester” omfatter følgende personer:

VERDENSØKONOMISK FORUM PROJEKTTEAM

Jesse McWaters
Projektleder, Disruptiv Innovation i Finansielle Tjenester

Giancarlo Bruno
Seniordirektør, chef for finansielle servicebrancher

Michael Drexler
Seniordirektør, chef for investorbrancher

PROFESSIONEL SERVICESUPPORT FRA DELOITTE

Rob Galaski
Projektrådgiver, Deloitte

Christine Robson
Hovedforfatter, Deloitte

Yderligere tak

Projektteamet udtrykker sin taknemmelighed til følgende personer for deres bidrag og støtte gennem hele projektet (i alfabetisk rækkefølge):

Faiza Harji
Alex Rinaldi
Sabrina Sdao

Og til:

Deloitte Greenhouse (Eventfacilitering og lokationsservice)
Niveau 39 (Lokationstjenester)
Værdiwebben (Eventfacilitering)

Machine Translated by Google

Resumé

Machine Translated by Google

Projektet "Blueprint for Digital Identity" er den seneste fase af forummets igangværende

Disruptiv innovation i arbejdet med finansielle tjenester

2015

FINANSIELLE TJENESTERS FREMTIDEN

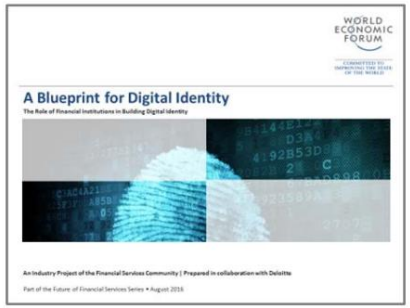
Projektet "Future of Financial Services" udforskede landskabet af disruptive innovationer inden for finansielle tjenester, leverede den første konsoliderede taksonomi for disse disruptioner og udforskede deres potentielle indvirkning på branchens struktur.

2016

UD OVER FINANSIELLE TJENESTERS FREMTID

Denne fase af det disruptive innovationsarbejde udforsker to emner med centralt potentiale som grundlæggende drivkræfter for fremtidig disruption.

En plan for digital identitet: Finansielle institutioners rolle i opbygningen af digital identitet



Dette projekt udforsker potentialet for digital identitet i finansielle tjenester og derudover og udarbejder en plan for implementering af effektive digitale identitetssystemer.

Fremtiden for finansiel infrastruktur: Et ambitiøst kig på, hvordan blockchain kan omforme finansielle tjenester

Dette projekt undersøger potentialet for distribueret ledger-teknologi til at transformere infrastrukturen i den finansielle servicesektor.

Machine Translated by Google

Mandatet for dette projekt var at udforske digital identitet og forstå den rolle, den spiller

Finansielle institutioner bør spille en rolle i opbygningen af en global standard for digital identitet

PROJEKTETS KONTEKST

Identitet er et kritisk emne inden for finansielle tjenester i dag. Nuværende identitetssystemer begrænser Fintech-innovation samt sikker og effektiv levering af tjenester inden for finansielle tjenester og samfundet mere generelt. Digital identitet er bredt anerkendt som det næste skridt inden for identitetssystemer. Men selvom der er mange bestræbelser i gang for at løse dele af identitetsudfordringen og skabe ægte digital identitet, er der behov for en samordnet og koordineret indsats for at opbygge et virkelig transformerende digitalt identitetssystem.

Dette dokument er tænkt som en vejledning til strategichefer i finansielle institutioner samt politiske beslutningstagere, der er interesserede i emnet identitet og ønsker at forstå den digitale identitet og deres egen potentielle rolle i skabelsen af robuste digitale identitetssystemer.

PROJEKTETS OMFANG

Mandatet for dette projekt var at udforske identitet og dens betydning inden for Fintech, finansielle tjenesteydelser og i udviklede samfund generelt, emnet digital identitet, og at give et overblik over de nuværende bestræbelser på at opbygge digitale identitetsløsninger.

Denne rapport vil diskutere forskellige strukturer for identitetssystemer og diskutere hvilke konfigurationer der er bedst egnede til at løse forskellige problemer, og give et perspektiv på finansielle institutioners rolle i opbygningen af digitale identitetssystemer.

Denne rapport vil ikke fokusere på at skabe standarder for identitet; der er allerede udført meget værdifuldt arbejde på dette område, og aktuelle udviklinger, såsom offentliggørelsen af Den Europæiske Unions eIDAS-forordning, bevæger samtalen på denne front. Den vil heller ikke diskutere teknologiske løsninger. Den vil snarere forsøge at skabe klarhed og retning omkring identitetsstrukturen og give en opfordring til finansielle institutioner til handling for at imødegå identitetsudfordringen.

Machine Translated by Google

Over 12 måneders research har vi samarbejdet med fageksperter gennem interviews og workshops med flere interessenter.

Brancheledere

Vejledning og tankelederskab fra **12 C-suite-ledere og 24 strategimedarbejdere** fra globale finansielle institutioner

Fageksperter

Personlige og telefoniske interviews med **over 100 fag- og brancheeksperter**

Globale workshops

Fire workshops med flere interessenter på globale finansielle knudepunkter med over 200 deltagere i alt, herunder brancheledere, innovatorer, fageksperter og regulatorer

Singapore
oktober 2015

New York, USA
november 2015

London, Storbritannien,
december 2016

Davos, Schweiz januar
2016

Machine Translated by Google

Denne rapport sammenfatter vores resultater og præsenterer et synspunkt på den rolle, vi ser for finansielle institutioner i digital identitet.

PROJEKTRESULTATER

Vores perspektiv: Finansielle institutioners rolle i digital identitet

Hvordan bør finansielle institutioner engagere sig i digital identitet? Hvilken rolle kan de spille i udviklingen af digitale identitetsløsninger?

1	**Indledning** Hvad er den globale identitetsudfordring, og hvilke problemer skaber den for finansielle institutioner?
2	**Digital identitetsgrundbog** Hvad er formålet med identitetssystemer, og hvorfor er digital identitet løsningen på den globale identitetsudfordring?
3	**Landskabet af digital identitet** Hvordan ser indsatsen for at opbygge digitale identitetssystemer ud globalt?
4	**Den rigtige løsning på det rigtige problem** Hvordan bør digitale identitetssystemer konstrueres for at imødekomme forskellige behov?
5	**Fordele ved digital identitet** Hvem vil drage fordel af introduktionen af digitale identitetssystemer?
6	**Implementering** Hvordan opnår man en global digital identitetsløsning?

Machine Translated by Google

Finanssektorens rolle
Institutioner inden for digital identitet

Machine Translated by Google

Nuværende identitetssystemer sætter store begrænsninger for Fintech-innovation

Manglende digital identitet begrænser udviklingen og leveringen af effektive, sikre og digitalt baserede Fintech-tilbud

Identitet er i øjeblikket et kritisk smertepunkt for Fintech-innovatører. Mange af disse innovatorer forsøger at levere rent digitale tilbud, men processen med at identificere brugere tvinger dem konsekvent til at bruge fysiske kanaler. Disse Fintech-innovatører ser nu udviklingen af en ny generation af digitale identitetssystemer som afgørende for fortsat innovation og levering af effektive, sikre og digitalbaserede Fintech-tilbud.

Eksempler

Betalinger

Betalinger kræver validering af ACH-oplysninger, hvilket betyder, at innovatorer inden for digitale betalinger enten skal kræve, at brugerne angiver identitetsoplysninger via pseudodigitale kanaler (f.eks. ved at fotografere deres kørekort) eller fungere som platforme oven på etablerede finansielle institutioner og stole på deres KYC. processer

Lån

Evaluering af kunderisiko og udstedelse af lån kræver validering af grundlæggende kundeoplysninger, hvilket kræver, at innovatorer indsamler oplysninger fra brugerne, igen gennem pseudodigitale kanaler såsom fotografering af eksisterende ID eller indsamling af pålidelige oplysninger fra en eksisterende kilde, og dermed decentralisering af en central del af produktudbuddet.

Machine Translated by Google

Digital identitet er en afgørende faktor for aktivitet inden for finansielle tjenester generelt

Digital identitet ville give finansielle institutioner mulighed for at udføre kritiske aktiviteter med øget nøjagtighed i forhold til den, der opnås ved fysisk identitet, og for at strømline og delvist eller fuldt ud automatisere mange processer.

Identitet er også centralt for den bredere finansielle servicebranche og muliggør levering af basale finansielle produkter og tjenester. Afhængighed af fysiske identitetsprotokoller introducerer ineffektivitet og fejl i disse processer. Digital identitet har et stort potentiale til at forbedre centrale finansielle serviceprocesser og åbne op for nye muligheder.

Eksempler

Operationelle beslutninger

Traditionelle FS-tilbud såsom forsikring og kredit samt kundeoplevelser såsom kontaktcentre og inkasso er afhængige af præcis og detaljeret viden om kunden.

Overholdelse af regler

Finansinstitutter er forpligtet til at overholde strenge regler for identifikation af deres kunder og er ansvarlige for fejl og unøjagtigheder.

Kundeoplevelse og produktlevering

Bedre viden om kundernes præferencer og vaner kan hjælpe FI'er med at levere en radikalt bedre kundeoplevelse (f.eks. skræddersy autentificeringskrav baseret på adfærd)

Machine Translated by Google

Relevansen af digital identitet rækker ud over finansielle tjenester til samfundet som helhed

Identitet muliggør mange samfundsmæssige transaktioner, hvilket gør stærke identitetssystemer afgørende for samfundets funktion som helhed.

Fysiske identitetssystemer udsætter i øjeblikket brugerne for risiko på grund af overeksponering af information og den høje risiko for informationstab eller -tyveri; de sætter også samfundet i fare på grund af potentialet for identitetstyveri, hvilket giver ulovlige aktører adgang til offentlige og private tjenester. Digital identitet ville strømline og forøge risikoen ved gennemførelsen af disse offentlige og private transaktioner.

OFFENTLIGE TRANSAKTIONER

Enheder skal bevise deres identitet eller bestemte egenskaber for at påvise deres berettigelse til offentlige tjenester.

Eksempler

- *Adgang til social bistand (f.eks. alderssikring, arbejdsløshedsforsikring)*
- *Adgang til uddannelse*
- *Adgang til sundhedspleje*
- *Adgang til samfundsstrukturer (f.eks. afstemning)*

PRIVATE TRANSAKTIONER

Enheder skal ofte bevise deres identitet eller bestemte egenskaber for at deltage i private transaktioner.

Eksempler

- *Mange basale handelstransaktioner (f.eks. køb af alkohol)*
- *Store transaktioner med private udbydere (f.eks. leje af en lejlighed, køb af bil)*

Machine Translated by Google

Behovet for digital identitet bliver stadig mere presserende

Fem nøgletendenser er et stigende behov for effektive og virkningsfulde identitetssystemer:

1

Stigende transaktionsvolumener
Antallet af identitetsafhængige transaktioner stiger gennem øget brug af digitale kanaler og øget konnektivitet mellem enheder.

2

Stigende transaktionskompleksitet
Transaktioner involverer i stigende grad meget forskellige enheder uden tidligere etablerede relationer (f.eks. kunder og virksomheder, der handler på tværs af grænser).

3

Stigende kundeforventninger
Kunderne forventer problemfri, omni-kanal servicelevering og vil migrere til tjenester, der tilbyder den bedste kundeoplevelse

4

Strengere lovgivningsmæssige krav
Tilsynsmyndigheder kræver øget gennemsigtighed omkring transaktioner, hvilket betyder, at finansielle institutioner kræver større granularitet og nøjagtighed i de identitetsoplysninger, de indsamler, og i stigende grad holdes ansvarlige for unøjagtige eller manglende identitetsoplysninger.

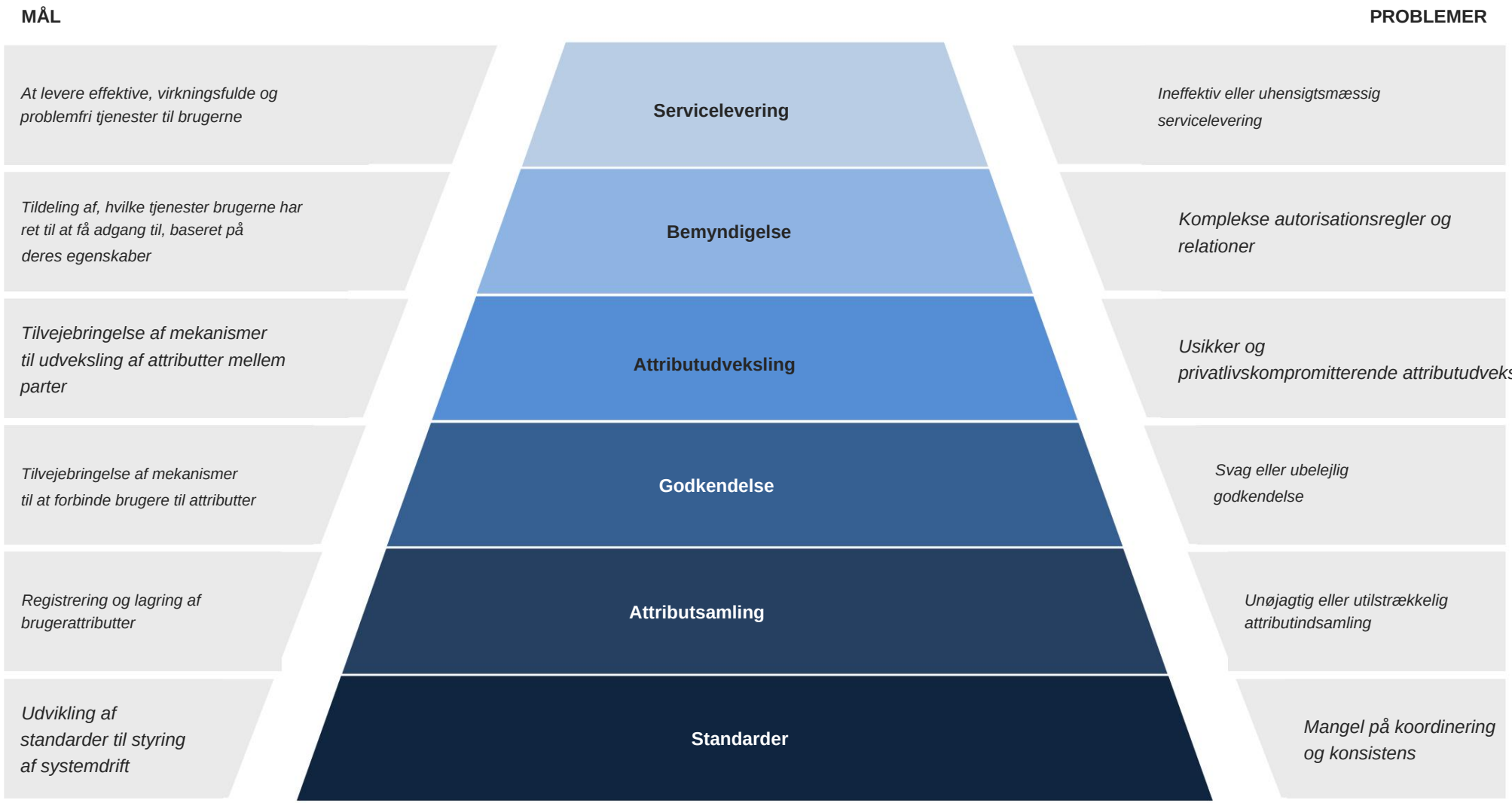
5

Øget hastighed på økonomisk/omdømmemæssig skade
Dårlige aktører i finansielle systemer bliver stadig mere sofistikerede i den teknologi og de værktøjer, de bruger til at udføre ulovlig aktivitet, hvilket øger deres evne til hurtigt at forårsage økonomisk og omdømmemæssig skade ved at udnytte svage identitetssystemer.

Machine Translated by Google

Identitet er imidlertid et problem med mange lag, der gør oprettelsen af digitale identitetssystemer kompleks.

Hvert lag af identitet tjener et forskelligt formål og lider af et særskilt sæt af problemer i nutidens identitetslandskab.



Machine Translated by Google

Der er i øjeblikket mange tydelige huller i det digitale identitetslandskab

1. Forveksling af autentificering med identitet

Mange bestræbelser i dag fokuserer på autentificering som en løsning på identitetsudfordringen uden at adressere styrken af de underliggende attributindsamlings- og godkendelsesprocesser • *Autentificeringsteknologiske*

løsninger er, selvom de er værdifulde, afhængige af eksisterende onboarding og attributindsamling processer

• *Godkendelsesløsninger leveret af globale teknologiplatforme er bekvemme for brugerne, men giver ikke sikkerhed eller verifikation af identiteten bag en konto eller et brugernavn*

2. Muliggørelse af transaktionsafslutning snarere end brugeraktivitet

Mange løsninger er drevet af målene og perspektiverne for en enkelt organisation og er derfor designet til at imødekomme behovene for bestemte transaktioner snarere end brugernes bredere behov • *E-forvaltningsløsninger*

har til formål at effektivisere leveringen af offentlige tjenester til brugerne og gør ikke muliggøre yderligere transaktioner, som brugerne måske ønsker at deltage i •

Transaktionsfokuserede løsninger resulterer i gentagen indsamling af 'tombstone'-data i stedet for effektive indsamling af brugercentrerede og risikorelevante data såsom transaktionsvaner

3. Opbygning af konsensus snarere end at fremme

handling Mange bestræbelser fokuserer på at opbygge enighed omkring standarder og processer snarere end at skabe en fuldstændig identitetsløsning og resulterer derfor ikke i løsninger, der kan implementeres i den

private sektor. • *Forsyningsvirksomheder og standardiseringsorganisationer fokuserer på at skabe konsensus og et standardiseret overblik over snarere end at tilbyde en komplet identitetsløsning*

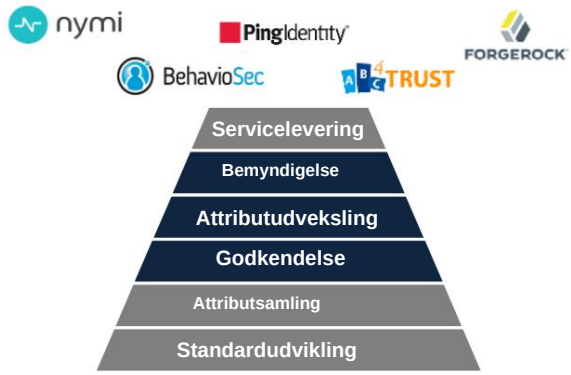
• *Tværstatslige indsatser har et betydeligt omfang, men er primært fokuseret på reguleringsniveau og ikke tilbyder kommercielt levedygtige løsninger*

Machine Translated by Google

Disse huller er et resultat af det overfyldte digitale identitetslandskab, hvor mange forskellige enheder bygger løsninger

Udbydere af teknologiløsninger

Udbydere af teknologiløsninger fokuserer på punktløsninger til autentificering, attributudveksling eller identitetsstyring for virksomheder



Private tjenesteudbydere

Private tjenesteudbydere fokuserer på at indsamle de attributter, de selv har brug for, for at levere specifikke tjenester til brugerne

Globale teknologivirksomheder

Globale teknologivirksomheder fungerer som platforme til at godkende brugere hos en bred vifte af andre tjenesteudbydere

Brancheorganisationer

Brancheorganisationer fokuserer på at standardisere og centralisere indsamlingen af attributter inden for den specifikke branche.

Regeringer

Regeringer fokuserer på at give deres borgere identitet og at tilbyde borgerne tjenester baseret på disse egenskaber.

Standardiseringsorganisationer

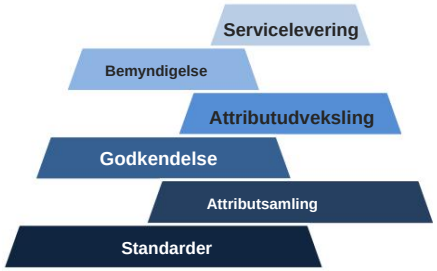
Standardiseringsorganisationer fokuserer på rammer og vejledning til udvikling af identitetssystemer

Machine Translated by Google

Der er åbning for nye digitale identitetssystemer, der kan levere omfang og skalering

Selvom mange igangværende bestræbelser, såsom nye autentificeringsløsninger, er afgørende for at opbygge digital identitet, er der et kernebehov for et stærkt system, der muliggør effektiv handling mod hvert lag af stakken.

Hele stakken behøver ikke at blive leveret af en enkelt enhed – nogle komponenter kan være modulære – men hele stakken skal være effektiv og integreret for at kunne levere digitale identitetssystemer, der har visse kritiske funktioner.



Kritiske karakteristika ved et stærkt identitetssystem

1 **Operationelt effektiv**
Systemet muliggør bekvem og effektiv gennemførelse af digitale transaktioner

2 **Omfang og skala**
Systemet muliggør store transaktionsvolumener ved at tilvejebringe transaktionskritiske attributter og forbinde store brugerantal med vigtige og ofte anvendte tjenesteudbydere

3 **Sikkerhed**
Systemet forhindrer, at brugeroplysninger bliver overeksponeret, mistet eller stjålet

4 **Brugerkontrol og privatliv**
Systemet giver brugerne mulighed for at bestemme, hvor deres oplysninger opbevares, og hvornår de deles eller eksponeres

5 **Levedygtighed**
Systemet leverer værdi til alle interessenter, skaber bred støtte og udbredelse og gør det til et kommercielt levedygtigt system

Machine Translated by Google

Finansielle institutioner er godt positioneret til at fremme oprettelsen af digitale identitetssystemer

Finansielle institutioner er exceptionelt godt positioneret til at drive identitetssystemer, der udfylder de huller, som den nuværende indsats har efterladt

STRUKTUREL

1	Finansielle institutioner fungerer allerede som **lagre af kundeattributter** til deres egne kommercielle formål og er derfor positioneret til at fungere som identitetsudbydere uden en omfattende inkrementel indsats.
2	Finansielle institutioner er en af meget få typer institutioner, der kan **verificere brugeroplysninger;** de udfører allerede denne funktion kommercielt og reguleringsformål
3	Finansielle institutioner har **incitamenter til at indsamle nøjagtige brugeroplysninger** til deres egne kommercielle formål
4	Finansinstitutter har **dokumenteret eksekveringsevne** til at udvikle nye systemer og standarder (f.eks. Interac), der er blevet bredt anvendt og effektivt anvendt i den private sektor
5	Finansbranchen har næsten fuldstændig **dækning af brugere** (personer, juridiske enheder og aktiver) i udviklede økonomier
6	Globale finansinstitutter har sammenkoblede **operationer på tværs af flere jurisdiktioner,** hvilket giver dem en strukturel fordel ved at muliggøre tværgående jurisdiktionelle identitetstransaktioner og -systemer

POSITIONERING

1	FI-drift og brug af kundedata er **strengt reguleret**
2	Finansielle institutioner fungerer som **etablerede formidlere** i mange transaktioner og er derfor godt positioneret til at fungere som identitetsformidlere
3	Finansielle institutioner har typisk **mere end blot forbrugernes tillid** til, at de er sikre opbevaringssteder for information og aktiver, udover andre institutioner.

Machine Translated by Google

Der er en stærk forretningsmæssig fordel for, at finansielle institutioner leder udviklingen af digitale identitetssystemer.

Finansinstitutter kan opnå betydelige fordele ved at investere i udviklingen af digitale identitetsløsninger. Vi har kategoriseret disse fordele i tre kategorier: effektivitet/ omkostningsbesparelse, nye indtægtsmuligheder og brandforbedring samt transformative fremtidige muligheder.

Effektivitet / Omkostningsbesparelse

Muligheder for at strømline nuværende processer, øge automatiseringen og reducere fejl og menneskelig indgriben

Nye indtægtsmuligheder

Muligheder for at skabe nye indtægtsstrømme fra nye produkter og tjenester og for at øge den positive genkendelse af brandet

Transformativ fremtidstilstand

Muligheder

Muligheder for at udvide din kerneforretning og dine kompetencer for at skabe transformative nye forretningsmodeller og nå nye kunder

Machine Translated by Google

Finansielle institutioner kunne drage fordel af grundlæggende effektivitetsforbedringer og omkostningsbesparelser…

Effektivitet / Omkostningsbesparelse

Proceseffektivisering og automatisering

Strømlin og forbedr onboarding- og compliance-processer gennem adgang til en pålidelig og konsolideret digital visning af brugerattributter, minimer RFI'er og informationsafhjælpning på grund af unøjagtigheder og menneskelige fejl.

Forbedret servicelevering

Tilbyde kunderne i stigende grad skræddersyede produkter og tjenester ved at udnytte utraditionelle egenskaber

Forbedr proceseffektiviteten og øg STP ved at automatisere processer gennem brug af standardiserede, pålidelige digitale data

Forbedret kundeoplevelse

Forbedre kundeoplevelsen ved at udnytte en række brugerattributter til bedre at forstå kundens behov og præferencer

Forbedret risikovurdering og scoring

Forbedre risikovurdering og reducer svindel ved at skabe mere holistiske og præcise kunderisikoprofiler, der kan informere om overvågning af mistænkelige transaktioner, forsikringsudbetalinger og levering af kredit- og risikobaserede produkter.

Machine Translated by Google

Udvikle nye indtægtsstrømme…

Nye indtægtsmuligheder

Nye finansielle produkter og tjenester

Tilbyde nye produkter og tjenester baseret på øget viden om kunderne (f.eks. udvidet finansiel rådgivning, nye forsikringsprodukter såsom forsikring på delvist ejede aktiver og adfærdsbaseret forsikring)

Identitet som en tjeneste

Tilbyd identitet som en tjeneste til afhængige parter, der ikke kan eller ikke ønsker at gemme kundeoplysninger

Kunder, der kun bruger identitet

Tilbyd identitet som en separat, gebyrbaseret tjeneste til personer, der ikke ellers handler med den pågældende finansielle institution

Machine Translated by Google

... og strække sig ud over den nuværende forretning og markeder for fundamentalt at transformere deres forretning

Muligheder for transformative fremtidige stater

Ansvarsfordeling Flyt
ansvaret for ukorrekte oplysninger og resultaterne af at opbevare disse oplysninger fra finansielle institutioner til andre enheder i netværket (f.eks. brugere gennem godkendelses- og samtykkekrav)

Trustmæglervirksomhed
Agere som en 'tillidsmægler' i tidligere tillidsløse interaktioner mellem forskellige parter i flere brancher, udvide FI'ers rækkevidde ud over FS-branchen og nå nye profitpuljer

Forstyrrelse af kreditbureaumodellen
Evaluer kundernes kreditværdighed baseret på nøjagtige identitetsdata, herunder præferencer og økonomisk historik, i stedet for at stole på tredjeparter og udvinding af flere forskellige datakilder.

Fokusering om kunden
Fokuser forretningen på kundeservice, bistå med den daglige beslutningstagning og udviske linjerne mellem finansiel og ikke-finansiel rådgivning.

Partnerskaber med den offentlige sektor
Bliv den betroede identitetsudbyder for den offentlige sektor, der hjælper med sociale ydelser og borgerlige krav såsom selvangivelse

Machine Translated by Google

Vi opfordrer finansinstitutter til at fremme udviklingen af digitale identitetssystemer

Finansielle institutioner bør fremme bestræbelserne på at opbygge digitale identitetssystemer og fremme opbygningen og implementeringen af identitetsplatforme gennem oprettelsen af et minimum af levedygtige digitale identitetssystemer.

Krav til et minimumsbrugbart identitetssystem

1 **Identitetsbestemmelse**

Identitetsudbyder(e), der besidder pålidelige oplysninger og dækker en kritisk masse af brugere inden for deres målområde, og som kan betjener derfor et stort antal brugere og transaktioner

2 **Attributter med høj transaktionsvolumen**

Sikker opbevaring af verificerede attributter, der kræves til almindelige transaktioner (iboende attributter såsom navn, fødselsdato, nationalitet , nationalt identifikationsnummer og nogle tildelte attributter såsom adresse)

3 **Adoption af den afhængige part**

Inddragelse af afhængige parter, der tilbyder vigtige og ofte anvendte brugervendte tjenester

4 **Teknologiplatform** En

teknologiplatform, der muliggør sikker attributudveksling mellem identitetsudbydere og afhængige parter med en bekvem samtykkemekanisme med brugere (f.eks. fungerer på mobil og desktop)

5 **Systemstandarder**

Tilsyns- og ansvarsstandarder, der styrer drift og brug af brugeroplysninger i systemet og fastsætter ansvars- og brugerbetingelser. Klagemuligheder

6 **Juridisk og regulatorisk accept**

Juridisk og lovgivningsmæssig accept af brug af tredjepartsverificerede oplysninger, attributudveksling og ekstern brug af brugeroplysninger

Machine Translated by Google

Finansielle institutioner kan anvende flere forskellige tilgange til at oprette identitetssystemer

Der findes forskellige konfigurationsmuligheder for udvikling af digitale identitetssystemer, hver med fordele og ulemper.

Enkeltinstitution

Globale institutioner kunne skabe interne systemer, der strækker sig på tværs af de jurisdiktioner, hvor de opererer

Dette ville muliggøre en hurtig implementering, men en enkelt institution ville sandsynligvis have svært ved at opnå en kritisk masse af brugere, hvilket ville begrænse dens evne til at drive systemadoption og integration af afhængige parter.

Konsortium

Konsortier af finansielle institutioner kunne danne netværk, der dækker store, afgrænsede oligopoløkonomier (såsom Canada eller Australien)

Et konsortium kræver en høj grad af samarbejde mellem parterne, men er en effektiv metode til at opnå fuldendt dækning over en brugergruppe

Konsortier er velegnede til at give identitet til enkeltpersoner, da datalagring ikke er centraliseret, hvilket øger privatlivets fred og systemets robusthed.

Forbrugsvarer

Finansielle institutioner kunne oprette brancheforsyningsvirksomheder til at levere identitetstjenester på tværs af branchen

Denne model er effektiv til at skabe standardisering og bred dækning, men implementeringen kan være vanskelig på grund af involvering af mange forskellige interessenter.

Forsyningsvirksomheder er en god model for identitet af juridiske enheder og aktiver, fordi de giver et standardiseret overblik og en gylden registrering af information

Machine Translated by Google

Denne rapport vil give vejledning i at konstruere effektive og robuste digitale identitetssystemer, samtidig med at man undgår implementeringsfælder.

Implementering af identitetssystemer er ekstremt følsomt og derfor let at begå fejl; situationsbestemte, operationelle og kulturelle faktorer har alle vigtige implikationer for identitetssystemer, og implementering eller operationel fiasko har ekstremt negative konsekvenser for både drivkræfterne bag identitetssystemer (f.eks. spild af ressourcer) og for brugerne (f.eks. databrud).

Vi har undersøgt landskabet for identitetsudbydere for at forstå, hvilke indsatser der er i gang, og hvilke systemmodeller der er bedst egnede til forskellige situationer, samt for at give anbefalinger til systemkonfiguration og implementering.

1. INDLEDNING

Introducerer den globale identitetsudfordring og hvordan problemer med identitet manifesterer sig for finansielle institutioner.

2. INSTRUKTION TIL DIGITAL IDENTITET

Opsummerer centrale begreber inden for digital identitet

3. DET DIGITALE LANDSKAB IDENTITETSSYSTEMER

Beskriver landskabet for digitale identitetsløsninger og introducerer et sæt arketyper, der repræsenterer det eksisterende sæt af løsninger.

4. DEN RIGTIGE LØSNING TIL DEN RIGTIGE PROBLEM

Diskuterer, hvordan identitetsløsninger bør konfigureres for at opnå succes

5. FORDELE VED DIGITAL IDENTITET

Introducerer de interessenter, der er involveret i et digitalt identitetsnetværk, og de typer fordele, som hver interessent kan opnå

6. IMPLEMENTERING, SAMMENKOBLING OG OPFORDRING TIL HANDLING

Fremhæver de næste skridt og de vigtigste interessenter, der skal involveres for at implementere et digitalt identitetsnetværk med succes

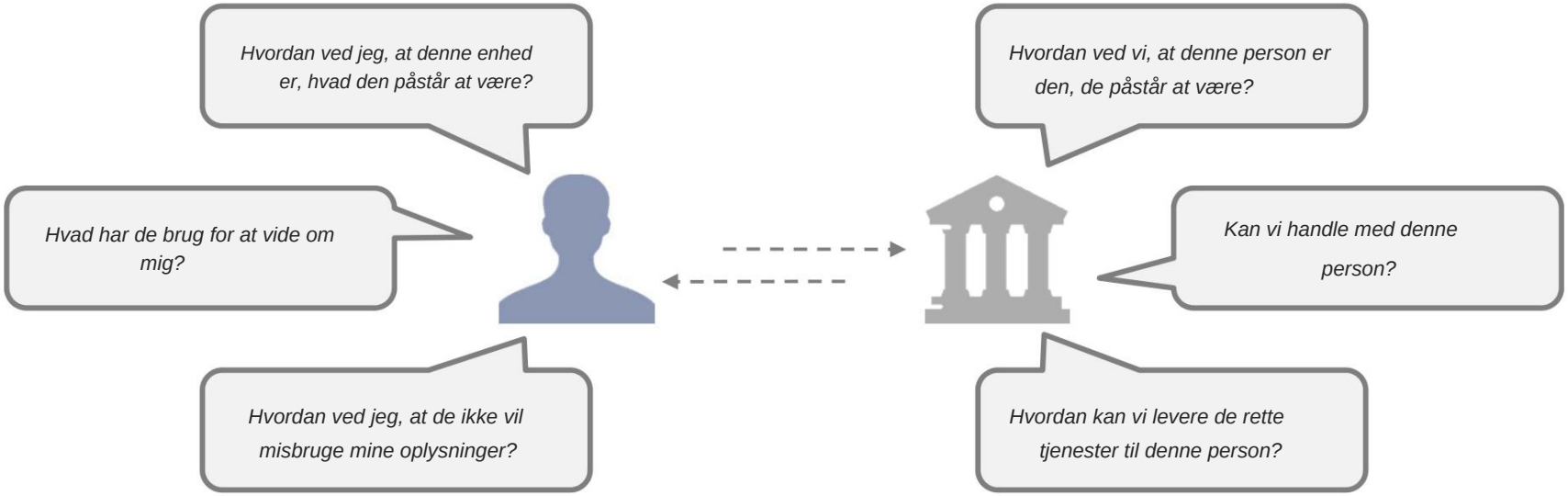
Machine Translated by Google

Den globale identitetsudfordring

Machine Translated by Google

Identitet er afgørende for dagens samfund

Identitet er fundamentalt for mange af de transaktioner, der finder sted i dagens samfund. I enhver udveksling med krav til de transaktionerende parter – de skal have en vis alder eller bo i en bestemt jurisdiktion – skal der være strukturer på plads, der giver enheder mulighed for at fastslå visse oplysninger om deres modpart og have tillid til, at oplysningerne er sande.



IDENTITETS ROLLE I TRANSAKTIONER

Mange transaktioner kræver ikke identitet. Nogle, såsom anmeldelse af kriminalitet, kan faktisk kræve anonymitet. Mange transaktioner kræver dog identitet: for at afgøre, om de nødvendige betingelser for, at transaktionen kan finde sted, for at etablere en relation til gentagne transaktioner eller for at skræddersy levering af produkter og tjenester.

Samfundet har brug for identitetssystemer, der muliggør identitetskrævende transaktioner i stor skala, og som implementerer metoder, der muliggør formel stilning og besvarelse af identitetsforespørgsler i stor skala, for at muliggøre mange daglige transaktioner.

Machine Translated by Google

Ineffektive identitetssystemer skaber globale udfordringer for mennesker, virksomheder og samfundet som helhed

Afhængighed af ældre identitetssystemer, der ikke effektivt muliggør de transaktioner, som personer og enheder ønsker at deltage i, skaber udfordringer for en bred vifte af interessenter.

FOR MENNESKER

Udelukkelse af tjenester

Enkeltpersoner er udelukket fra nøgletjenester på grund af deres manglende evne til at dokumentere identitet

Dårlig brugeroplevelse

Tjenester leveret til brugerne matcher ikke deres behov eller leveres ubelejligt

Overeksponering af information

Brugeroplysninger er overeksponeret, hvilket sætter brugerne i risiko for identitetstyveri og brud på privatlivets fred

Procesineffektivitet

Bevis for identitet involverer mange trin og dokumenter

FOR VIRKSOMHEDER

Ineffektiv servicelevering

Brugervendte processer er besværlige, hvilket resulterer i en dårlig kundeoplevelse

Uklar risiko

Manglende pålidelig information forhindrer virksomheder i at beregne risikoen ved at drive forretning præcist

Svig

Virksomheder lider under svindel som følge af stjålne eller ukorrekte kundeoplysninger eller dårlig autentificering

Procesineffektivitet

Processer leverer forældede data eller kræver kontrol af flere kilder

FOR SAMFUNDET

Udelukkelse af tjenester

Enheder kan muligvis ikke bevise attributter og er derfor udelukket fra centrale sociale strukturer.

Serviceuoverensstemmelse

Tjenesterne leveres forkert på grund af manglende information

Svig

Enheder kan bruge falske oplysninger eller fordreje oplysninger til at få ulovlig adgang til tjenester

Procesineffektivitet

Processer er i høj grad manuelle og papirbaserede, hvilket kræver menneskelig indgriben og afhjælpning.

Machine Translated by Google

Disse globale identitetsudfordringer manifesterer sig som specifikke forretningsproblemer for FI'er

Identitet er afgørende for FI'er; deres forretning er udelukkende transaktionsbaseret og involverer transaktioner med en høj grad af risiko og kræver en høj grad af sikkerhed i forbindelse med gennemførelse. Globale problemer med identitet manifesterer sig derfor som specifikke forretningsproblemer for FI'er.

ILLUSTRATIV: FORRETNINGSPROBLEMER INDEN FOR FINANSIELLE TJENESTER

Forretningsproblem	Detailbankvirksomhed / små og mellemstore virksomheder	Erhvervs- og investeringsbankvirksomhe
Ineffektive og dyre onboardingprocesser	✓	✓
Ineffektive, dyre og ineffektive kend-din-kunde (KYC) og due diligence-processer	✓	✓
Meget manuelle og tidskrævende compliance-processer	✓	✓
Vanskeligheder med at samle oplysninger om juridiske enheder og bestemme den samlede risikoeksponering	✓	✓
Vanskeligheder med at knytte individuel identitet (f.eks. virksomhedsdirektører) til virksomhedsidentiteter	✓	✓
Vanskeligheder med at identificere alle transaktionsmodparter (f.eks. tredjeparter i handelsrelationer)	✓	✓
Vanskeligheder med at overholde lovgivningsmæssige standarder omkring datahåndtering og privatliv	✓	✓
Flere visninger af kunden	✓	✓
Vanskeligheder med at levere effektive/egnede produkter og tjenester	✓	
Manglende indsigt i den økonomiske historik for nye kunder	✓	
Høje svindelrater	✓	
Vanskeligheder med at spore aktivernes oprindelse og ejerskab		✓
Vanskeligheder med at overvåge og spore genpantsættelse af aktiver		✓

Machine Translated by Google

Mange af disse udfordringer er drevet af brugen af fysiske identitetsprotokoller til at håndtere digitale transaktioner.

Dagens standardidentitetssystemer er baseret på fysiske dokumenter og processer, hvilket skaber mange begrænsninger.

KARAKTERISTIKA FOR FYSISKE IDENTITETSSYSTEMER

Dokumentbaseret: Identitet er baseret på fysiske optegnelser – evnen til at bevise identitet afhænger af adgang til og autentificering af fysiske dokumenter (f.eks. pas, ID-kort og optegnelser)

Silobaseret: Identitetsoplysninger opbevares på separate steder, der ikke er sammenkoblede og ikke muliggør aggregering, hvilket kan være ønsket af enheden selv eller påkrævet for visse applikationer.

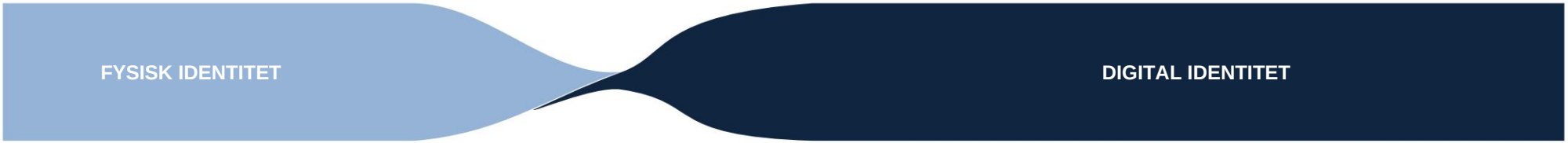
Ufleksibel: Identitet er kodificeret i dokumenter som et begrænset og standardiseret sæt af oplysninger om en enhed, der ikke let kan tilpasses transaktionskrav.

PROBLEMERNE MED FYSISK IDENTITET

- *Bevis for identitet baseret på besiddelse af fysiske midler*
  Dokumenter kræver muligvis ikke påvisning af en forbindelse mellem en person og dokumenterne (dvs. godkendelse), hvilket muliggør brug af en enheds legitimationsoplysninger af en anden bruger.
- *Fysiske identitetsdokumenter kan forfalskes, ændres eller manipuleres, samt mistes eller stjåles*
- *Præsentation og overførsel af fysiske attributter skaber potentiale for menneskelige fejl i transaktioner*

IDENTITETSSKIFTET

Identitet er nu ved et vendepunkt; fysiske identitetssystemer bryder sammen, og digitale systemer dukker op som reaktion.



Fysisk identitet *blev designet til at muliggøre ansigt-til-ansigt transaktioner mellem enheder*

Den digitale økonomi *ændrer den måde, identitetstransaktioner finder sted på*

Digital identitet *muliggør transaktioner i den digitale verden og tilbyder forbedret funktionalitet for brugerne*

Machine Translated by Google

Digitale identitetssystemer understøtter behovene i nutidens verden

Digitale identitetssystemer opstod som et direkte svar på kravene til transaktioner i den digitale verden.

KARAKTERISTIKA VED DIGITALE IDENTITETSSYSTEMER

Digitalbaseret: Identitet eksisterer som et sæt digitale poster, som brugeren kan kontrollere og bruge til at gennemføre transaktioner.

Sammenkoblet: Bevis for identitet kan kommunikeres mellem enheder i et standardiseret, digitalt format

Fleksibelt: Identitetssystemer tilpasser sig transaktionens karakter og tilpasser sig løbende kravene ved at integrere yderligere information for at skabe et omfattende overblik over brugeren.

LØFTE OM DIGITAL IDENTITET

- *Digital information kan beskyttes mod skader, manipulation, tab og tyveri med avancerede godkendelses- og sikkerhedsprotokoller*
- *Digital information kan deles på strømlinede, skræddersyede og sikre måder, baseret på brugerens samtykke*
- *Institutioner kan bedre kende og betjene deres kunder, forbedring af eksisterende produkter og tilbud af nye produkter og tjenester til de underprivilegerede*

FORDELE

Digital identitet ville give en række fordele for mennesker, virksomheder og samfundet.

Privatliv og kontrol
Folk ville kunne kontrollere adgangen til deres oplysninger

Omsætningsvækst
Finansielle institutioner ville have muligheder for at tilbyde identitet som en tjeneste

Forbedret overholdelse
Regulatorer ville have øget adgang til pålidelige, opdaterede oplysninger

Forbedret servicelevering
Regeringer kunne lettere og mere effektivt levere offentlige tjenester

Machine Translated by Google

Nye og modne teknologier har vigtige konsekvenser for skabelsen af robuste digitale identitetssystemer

Disse teknologier kan rumme et betydeligt potentiale for identitet og bliver udforsket af mange forskellige aktører.

Datalagring

Nye teknologier kan tilbyde forbedrede metoder til lagring af brugeroplysninger og øge brugerkontrol, privatliv og sikkerhed

- Distribueret Ledger-teknologi kombineret med kryptering og cloud-lagring gør det muligt at opbevare og overføre information punkt-til-punkt i et spredt, uforanderligt netværk
- Fødererede identitetsstandarder, såsom SAML 2.0, skaber interoperabilitet mellem identitetsstyringsnetværk og eksterne applikationer, hvilket gør det muligt for fødererede identitetssystemer at skalere til et stort antal identitetsudbydere og afhængige parter.

Dataoverførsel

Forbedrede attributudvekslingsprotokoller gør det muligt at dele information sikkert mellem slutpunkter uden risiko for aflytning eller dekryptering, og med flere kontroller, der skaber privatliv for brugerne.

- Forbedrede krypteringsprotokoller, såsom Keyless Signature Infrastructure på blockchainen og hashing, giver stærke beskyttelse af følsomme oplysninger og øge pålideligheden af digitale aktiviteter
- Dataoverførselsprotokoller, såsom Attributed Based Credentials 4 Trust og nul-vidensbeviser, forhindrer oprettelsen af metadata ved at skjule transaktionsslutpunkter, hvilket øger brugernes privatliv

Godkendelse

Mange nye teknikker til brugergodkendelse undersøges for at øge informationssikkerheden og brugerkontrollen under visse omstændigheder ved at forbinde brugerne til deres digitale aktiviteter på mere robuste og vedvarende måder.

- Adfærdsmæssig og kontekstuel godkendelse inkorporerer menneskelige og miljømæssige faktorer for at godkende en bruger eller enhed
- Biometri, herunder fingeraftryk, nethindescanning, hjerteslagsbølgeform og ansigtsgenkendelse baseret på mobile enheder, har potentiale til at give større bekvemmelighed og sikkerhed og integreres i mange kontroller mod svindel

Machine Translated by Google

Digitale identitetssystemer har et stort potentiale, men også mange faldgruber i implementeringen

Mange nye identitetssystemer er under udvikling verden over som svar på behovet for digital identitet og nye teknologiske muligheder. Imidlertid har ikke alle været succesfulde, hvilket illustrerer nogle af de faldgruber, der er forbundet med konstruktionen af identitetssystemer.

FALDGRUBBER I IDENTITETSSYSTEMER

Afvisning fra interessenter

- Brugere implementerer muligvis ikke systemet på grund af dårligt design eller mistillid til systemets formål eller struktur
- Interessenter kan opfatte systemer med begrænset omfang og skala som værdiløse, og derfor ikke anvende dem

Ineffektiv teknologi • En dårlig teknologiplatform kan reducere systemfunktionaliteten og forhindre brugerintegration eller fuldførelse af transaktioner

- Utilstrækkelig databeskyttelse resulterer i brud og systemkompromittering og datalækage

Begrænset støtte • Systemer, der har støtte fra et snævert interesseområde, kan fejle på grund af inkonsekvent indsats bag deres konstruktion og drift

- Systemer, der mangler støtte fra alle vigtige interessenter, oplever muligvis ikke bæredygtig og kontinuerlig implementering

Uholdbar drift • Systemer med uholdbare drifts- eller forretningsmodeller vil fejle

Politiske ændringer • Store, komplekse og følelsesladede programmer såsom ID-kort kan være modtagelige for politiske og/eller ideologiske ændringer

Eksempler på udfordringer i identitetssystemer er almindelige…

Hack Brief: Tyrkiet-brud afslører information om mere end Halvdelen af dens borgere

-WIRED, april 2016

Filippinske valgrekorder brudt i 'største regeringshack nogensinde'

The Guardian, april 2016

Aadhaar-lovforslag vedtaget i Lok Sabha, oppositionen frygter 'overvågning'

-Indian Express, marts 2016

Sydkorea ved en korsvej med tab af ID-kort og datatyveri

CBC News, oktober 2014

Ordningen med nationale identitetskort [i Storbritannien] vil blive afskaffet inden for 100 dage, og alle kort vil blive ugyldige.

-BBC Nyheder, maj 2010

Machine Translated by Google

Identitetsgrundlægger

Machine Translated by Google

Hvorfor er identitet vigtig?

Identitet er grænsen for privatliv og sikkerhed

i den digitale verden

I en stadig mere grænseløs og digital verden, privatliv og Sikkerhed kan ikke garanteres ved at bygge mure omkring følsomme oplysninger

Identitet er den nye grænse for privatliv og sikkerhed, hvor selve enhedernes natur er det, der gør det muligt for dem at fuldføre nogle transaktioner, men blive nægtet adgang til at gennemføre andre

At forstå vigtigheden af identitet og dens kritiske betydning stærke identitetsprotokoller, der beskytter mod cyberrisiko og retssager behovene hos transaktionsparterne er det vigtigt at forstå, hvad identitet er, og dens rolle i at muliggøre transaktioner

9-cifrede aftaler løfter cybersikkerheden

Investeringer til et rekordhøjt niveau

-Forbes, februar 2016

Cybersikkerhed øverst på regeringens dagsorden

Times of India, februar 2016

I dagens æra med databrud, er du sikker på, at dine data er beskyttet?

-Sikkerhedsefterretninger, januar 2016

1 ud af 3 amerikanere offer for databrud i sundhedsvæsenet i 2015

Informationsstyring, februar 2016

USA presser detailbanker til at hjælpe millioner af 'bankløse' amerikanere

-Reuters, februar 2016

Sådan bekæmper du identitetstyveri på skatteområdet

-Huffington Post, februar 2016

FCA ilægger Barclays en bøde på 72 millioner pund for dårlig håndtering af risici vedrørende økonomisk kriminalitet

-Automatiseret Trader, november 2015

Machine Translated by Google

Identitet er en samling af informationer, der beskriver en enhed

Identitet er ikke en monolit; det er en samling af individuelle attributter, der beskriver en enhed og bestemmer de transaktioner, som denne enhed kan deltage i. Selvom det samlede eksisterende sæt af attributter er uendeligt, kan de bredt kategoriseres i tre grupper: iboende, nedarvede og tildelte attributter. Disse attributter er forskellige for medlemmer af tre hovedbrugergrupper: enkeltpersoner, juridiske enheder og aktiver.

	For enkeltpersoner:	For juridiske enheder:	For aktiver:
IBOENDE ATTRIBUTTER Attributter, der er iboende for en enhed og ikke er defineret af relationer til eksterne enheder.	• *Alder* • *Højde* • *Fødselsdato* • *Fingeraftryk*	• *Industri* • *Virksomhedsstatus*	• *Aktivets art* • *Udsteder af aktiver*
AKKUMULEREDE ATTRIBUTTER Attributter, der indsamles eller udvikles over tid. Disse attributter kan ændre sig flere gange eller udvikle sig i løbet af en enheds levetid.	• *Sundhedsjournaler* • *Præferencer og adfærd (f.eks. telefonmetadata)*	• *Forretningshistorik* • *Juridisk registrering*	• *Ejerskabshistorik* • *Transaktionshistorik*
TILDELTE ATTRIBUTTER Attributter, der er knyttet til enheden, men som ikke er relateret til dens iboende natur. Disse attributter kan ændre sig og afspejler generelt de relationer, som enheden har til andre kroppe.	• *Nationalt identifikationsnummer* • *Telefonnummer* • *E-mailadresse*	• *Identifikationsnumre* • *Jurisdiktion* • *Direktører*	• *Identifikationsnumre* • *Forvaltning*

Machine Translated by Google

Specifikke attributter gør det muligt for enheder at gennemføre bestemte transaktioner

Identitet er det samlede sæt af en enheds attributter. Disse attributter gør det muligt for enheder at deltage i transaktioner ved at bevise over for deres modpart, at de har de specifikke attributter, der kræves til den pågældende transaktion.

EKSEMPEL: Brugere og transaktioner

Enkeltpersoner	Juridiske enheder	Aktiver
For at købe alkohol skal brugerne bevise, at de er over den lovlige alder for alkoholforbrug i den pågældende jurisdiktion.	*For at blive onboardet hos en FI skal enheden have bevis for, at den er en juridisk og ikke-sanktioneret enhed*	*Handel med aktiver, såsom handel med aktier på en børs, kræver bevis for ejerskab og oprindelse*
For at stemme skal brugerne bevise, at de er over den lovlige stemmeretsalder, har statsborgerskab og bor i den pågældende jurisdiktion.	*For at kunne handle på kapitalmarkederne skal enheden have bevis for, at den er en juridisk og ikke-sanktioneret enhed med en acceptabel risikoprofil.*	*Overdragelse af ejendomsretten til et aktiv kræver bevis for ejerskab fra den enhed, der overfører aktivet*
For at åbne en bankkonto skal brugerne bevise, at de er en ikke-godkendt person, der har lovlig tilladelse til at foretage finansielle transaktioner.		

Bemærk: Aktiver har identitet, men kan ikke handle eller foretage transaktioner på egen hånd. Aktiver kræver depotbanker, der er berettiget til at handle eller foretage transaktioner på aktivets vegne.

Machine Translated by Google

Identitetstransaktioner har tre hovedaspekter

Bemyndigelse	***Attributter***	***Godkendelse***
Hvad skal være sandt om brugerne for at gennemføre den ønskede transaktion?	*Kan brugerne bevise, at de er berettigede til at gennemføre denne transaktion?*	*Tilhører de præsenterede egenskaber virkelig den enhed, der præsenterer dem?*
Autorisation er en funktion af transaktionen og transaktionsmodparten; de vil bestemme kravene til transaktionsberettigelse og foretage en forespørgsel om bestemte brugerattributter (f.eks. alder, adresse).	Brugere skal fremvise deres bevis for attributter som svar på forespørgslen. Når brugerne har fremvist de nødvendige attributter, skal modparten afgøre, om de er pålidelige.	Modparten vil afgøre, om attributterne matcher de præsenterede brugere. Hvis brugerne er i stand til at godkende attributterne, kan transaktionen fortsætte.

Gentagne identitetstransaktioner

Denne model for identitetstransaktioner gælder for onboarding-transaktioner, dvs. transaktioner, hvor modparterne ikke har en etableret relation, eller hvor modparten skal indsamle identitetsoplysninger ved hver transaktion.

Nogle identitetsrelationer kan have en enkelt onboarding-transaktion; efter initial onboarding af brugerne og verificering af dem gennem en fuld identitetstransaktion, kan modparten bruge en godkendelsesmetode (f.eks. brugernavn og adgangskode, chip-og-PIN-kort) til hver efterfølgende transaktion. Dette giver dem mulighed for at verificere, at den samme enhed udfører transaktionen hver gang uden at skulle gennemgå den fulde identitetstransaktionsproces.

*Bemærk: Ikke alle transaktioner kræver **præcis kendskab** til attributter. Mange transaktioner kræver blot, at attributdata falder inden for bestemte parametre (f.eks. i stedet for at kende en persons fødselsdato kræver en transaktion muligvis kun, at brugeren er over en bestemt alder); dette er afgørende for at konstruere privatlivsfremmende identitetssystemer.*

Machine Translated by Google

Forskellige identitetstransaktioner kræver forskellige niveauer af sikkerhed

Sikkerhedsniveauet (LoA) i en identitetstransaktion er den grad af sikkerhed, som de transaktionerende parter har for sandfærdigheden af den præsenterede identitet.

FORSIKRING I TRANSAKTIONER

En høj LoA i identitetstransaktioner er ikke altid ønskelig, da en høj LoA kræver intensiv onboarding og stærke autentificeringsprocesser, der kan være besværlige for brugeren. Den LoA, der kræves i en identitetstransaktion, bør derfor generelt afhænge af risiko – transaktionens risikoniveau og konsekvenserne af fejl.

FASTSÆTTELSE AF SIKKERHEDSNIVEAUER

Sikkerhedsniveauet for en given transaktion bestemmes af to hovedfaktorer: 1. Registreringsprotokoller:

Hvor strengt identitetsudbyderen verificerer attributter ved onboarding af brugere 2. Godkendelsesmetode: Styrken af den

godkendelsesmetode, der bruges til at gennemføre transaktioner mellem identitetsudbyderen

og den pårørende

Transaktioner med lav sikkerhed

Transaktioner, der ikke involverer frigivelse af information, men kun involverer en informationsstrøm fra brugeren til den afhængige part, er transaktioner med lav sikkerhed.

Eksempler omfatter onlineregistreringer (f.eks. tilmelding til en nyhedsside) og visse betalinger (f.eks. betaling af en parkeringsbøde online)

Transaktioner med høj sikkerhed

Transaktioner, der involverer frigivelse af følsomme og private oplysninger eller overførsel af penge eller aktiver, er transaktioner med høj sikkerhed.

Eksempler omfatter bank- og andre finansielle transaktioner, såsom brug af en online mæglerkonto og mange offentlige tjenester

Machine Translated by Google

Identitetssystemer har en tendens til at udvikle sig inden for naturlige grænser ...

Identitet eksisterer inden for netværk, der muliggør transaktioner mellem enhederne inden for netværket. Disse netværk har en tendens til at udvikle sig omkring brugergrupper med lignende behov og karakteristika. Disse grænser danner det, der kaldes "naturlige identitetsnetværk". Hvert naturligt identitetsnetværk har forskellige behov og kræver derfor forskellige systemkonfigurationer.

NATURLIGE IDENTITETSNETVÆRK

De netværk, der dannes inden for de naturlige grænser af identitetssystemer for individer, er baseret på **geografisk placering** eller **tilknytning til en tilsynsførende enhed.**

Eksempler omfatter nationale identitetssystemer, statslige eller provinsielle identitetssystemer og medarbejderstyringssystemer

De netværk, der dannes inden for de naturlige grænser af identitetssystemer for juridiske enheder, er baseret på **national tilhørsforhold, branche** eller **geografisk rækkevidde.**

Eksempler omfatter nationale eller globale virksomhedsregistre og brancheidentifikationssystemer

De netværk, der dannes inden for de naturlige grænser af identitetssystemer for aktiver, er baseret på deres **aktivklasse, oprindelse** eller **ejerskab.**

Eksempler omfatter registre over aktiver i en enkelt klasse eller registre over aktiver, der alle ejes af en enkelt enhed.

Machine Translated by Google

... og opererer på en grundlæggende fælles struktur

Formålet med et formelt identitetssystem er at give modparter uden et tidligere etableret forhold mulighed for at deltage i betroede transaktioner.

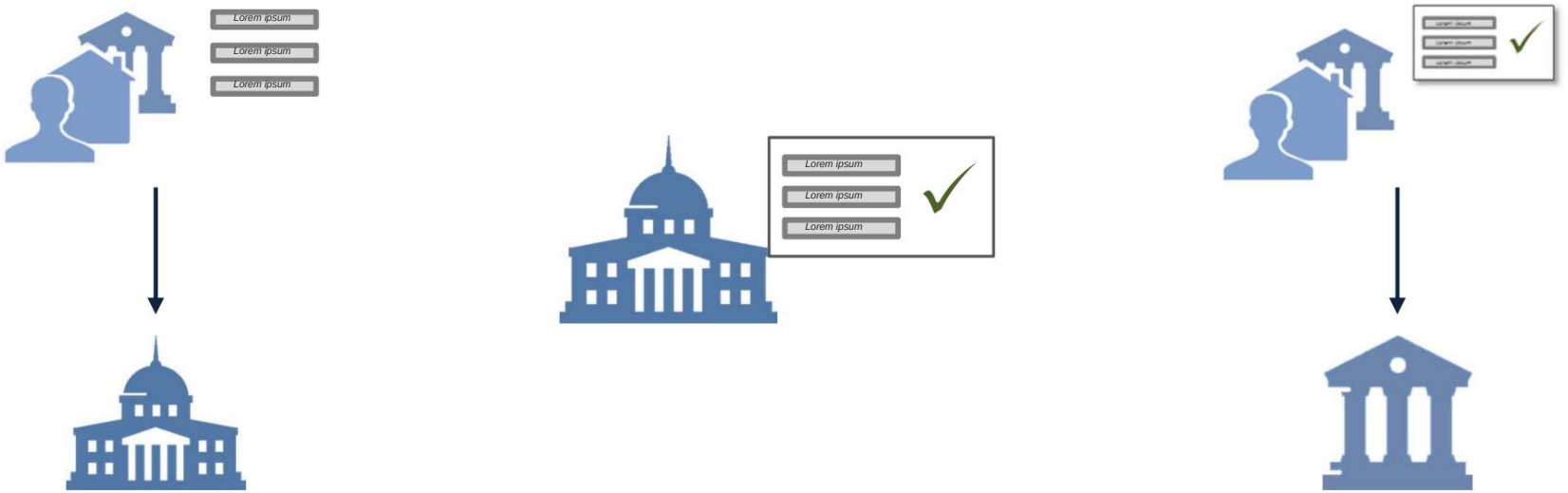
• I et formelt identitetssystem attesteres brugernes attributter af betroede tredjeparter; disse tredjeparter udsteder legitimationsoplysninger, der knytter deres attestering til de specifikke attributter med en metode til at autentificere legitimationsoplysningerne til den enhed, der præsenterer dem. • Brugere kan bruge deres tegnebog med legitimationsoplysninger til at deltage i transaktioner med andre enheder, der kræver bevis for eller viden om deres attributter

STRUKTUREN AF IDENTITETSSYSTEMER

1 *Brugeren præsenterer et sæt attributter for en tredjepart*

2 *Tredjeparten verificerer attributterne og knytter sin attestation til attributterne og bliver dermed identitetsudbyder for brugeren.*

3 *Brugeren bruger derefter legitimationsoplysningerne fra identitetsudbyderen i transaktioner med afhængige parter*



Machine Translated by Google

Visse roller og funktioner skal eksistere i ethvert identitetssystem

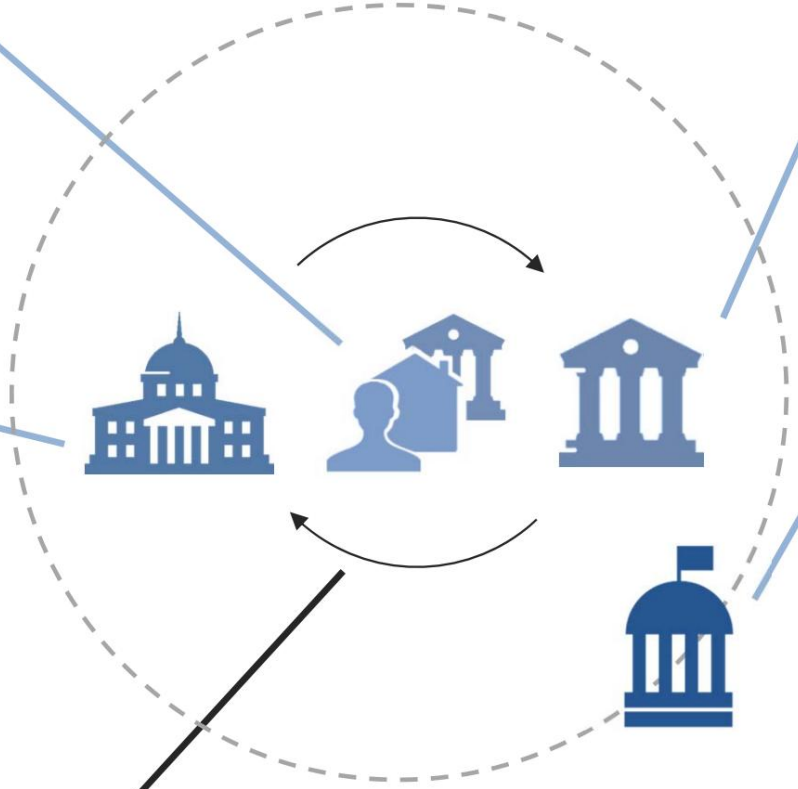
Ethvert identitetssystem skal have fire roller og én funktion for at fungere.

Brugere

Brugere er enheder, som systemet angiver identitet for, med det formål at give dem mulighed for at deltage i transaktioner.

Identitetsudbydere

Identitetsudbydere (IdP'er) er enheder, der besidder brugerattributter, bekræfter deres sandfærdighed og gennemfører identitetstransaktioner på vegne af brugere.



Forladte parter

Afhængige parter (RP'er) er enheder, der accepterer attestationer fra identitetsudbydere om brugeridentitet for at give brugerne adgang til deres tjenester.

Styringsorgan

Styringsorganet sørger for tilsyn med systemets overholdelse af systemadgangsregler og krav.

Attributudvekslingsplatform

Attributudvekslingsplatformen fuldfører transaktioner ved at matche identitetsforespørgsler fra RP'er med attributter fra IdP'er og udveksle attributter eller bevis for identitet.

Rolle

Fungere

Machine Translated by Google

Metoderne har udviklet sig, men konceptet med identitetssikring har ikke ændret sig over tid.

Det grundlæggende koncept, formålet og strukturen bag identitetssystemer har ikke ændret sig over tid, mens metoder og teknologi har gjort store fremskridt fremad.

Forbi → **Nuværende**

Et introduktionsbrev er en af de ældste former for identitetsdokumentation.

- **Bruger:** Enkeltpersoner ville bruge et introduktionsbrev som en bevis på identitet og karakter for en person, de ikke kendte
- **IdP:** Brevskriverne ville fremlægge attester for forskellige brugernes egenskaber (f.eks. at brugeren var en person med god karakter)
- **RP:** Modtagerne af brevet ville vælge, om de ville at acceptere attestationerne baseret på deres kendskab til IdP og deres evaluering af brevets sandfærdighed

I dag er et pas udstedt af en persons bopæls- eller oprindelsesland et af de mest almindelige og pålidelige identitetsdokumenter.

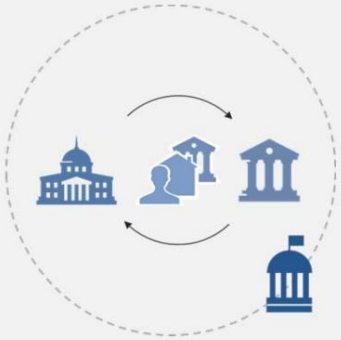
- **Bruger:** Enkeltpersoner bliver ofte bedt om at fremvise deres pas for at gennemføre transaktioner, der kræver bevis for identitet (f.eks. indrejse i nye lande, åbning af en bankkonto osv.).
- **IdP:** Landets regering fungerer som en IdP, hvilket gør visse attester om brugeren
- **RP:** Attestationer foretaget af IdP'en accepteres af en RP baseret på dens tillid til dokumentet, dets udsteder og dens vurdering af, om indehaveren er den reelle ejer af passet

Machine Translated by Google

Digital identitet gør det muligt at gennemføre identitetstransaktioner via digitale kanaler

Et digitalt identitetssystem har den samme grundlæggende struktur som et fysisk identitetssystem, men lagring og udveksling af attributter er fuldstændig digital, hvilket fjerner afhængigheden af fysiske dokumenter og manuelle processer.

FUNKTIONER VED DIGITALE IDENTITETSSYSTEMER



Digital informationslagring og -overførsel

- Brugeridentitetsoplysninger indsamles og lagres digitalt
- Brugeridentitetsoplysninger overføres mellem IdP'er og RP'er i digital form
- Formfaktorer, såsom computere eller mobile enheder i stedet for fysiske dokumenter, kan bruges til at gennemføre transaktioner

Direkte forbindelse

- Informationsoverførsel sker direkte mellem IdP'er og RP'er uden mellemmand (selvom brugerens samtykke kan indbygges) og uden manuel indgriben (f.eks. fysisk informationsindtastning)

DET NUVÆRENDE LANDSKAB FOR DIGITAL IDENTITET

Digital identitet er ikke et nyt koncept; der findes mange identitetssystemer i verden i dag, som enten inkorporerer nogle digitale elementer eller er udelukkende digitalt baserede systemer. Landskabet af digitale identitetsløsninger udforskes yderligere i næste afsnit af denne rapport. Disse systemer findes i et spektrum af modenhed og grad af sofistikering; dog er alle designet til at indfange nogle af de fordele, som digital identitet bringer i forhold til traditionelle fysisk baserede identitetssystemer.

Machine Translated by Google

Digital identitet tilbyder betydelige fordele i forhold til fysiske identitetssystemer

Ud over at tilbyde ny funktionalitet har digital identitet betydelige funktionelle fordele i forhold til fysisk baserede identitetssystemer.

Sikkerhed

ÿ Fysiske identitetsdokumenter kan let mistes, stjæles eller replikeres af ulovlige aktører, samt læses af enheder uden legitim grund til at have brugeroplysningerne

ÿ Digitale identitetsoplysninger kan lagres, overføres og eksponeres ved hjælp af banebrydende digitale sikkerhedsprotokoller, der ville forhindre databrud, ændring, tab og tyveri

Privatliv og kontrol ÿ

Fysisk identitet tillader ikke, at frigivelsen af oplysninger tilpasses identitetstransaktionen; identitetsdokumenter vise et fast sæt af oplysninger, der kan læses af næsten enhver enhed

ÿ Digital identitet giver enkeltpersoner mulighed for at kontrollere delingen af deres oplysninger og dermed eksponere den mindst mulige mængde information kræves for en given transaktion, og beskytte deres oplysninger mod ulovlig adgang

Brugeroplevelse

ÿ Fysisk identitet kræver, at brugerne manuelt viser dokumenter eller indtaster identitetsoplysninger i transaktioner, hvilket resulterer i en besværlig brugeroplevelse og skaber potentiale for menneskelige fejl i transaktioner

Digital informationsoverførsel ville strømline transaktionsprocessen for brugere og RP'er på tværs af alle kanaler, hvilket ville gøre det nemmere for begge parter at gennemføre transaktioner og fjerne risikoen for menneskelige fejl.

Fleksibilitet

ÿ Fysisk identitet resulterer i krystallisering af brugeridentitet i fysiske dokumenter og et fastlåst syn på identitet, der ikke kan udvides til at dække yderligere brugerattributter

ÿ Digital identitet ville give et fleksibelt og skalerbart system, der kunne inkorporere en større rigdom af identitet information end det, der er muligt i øjeblikket

Machine Translated by Google

Det digitale landskab
Identitetssystemer

Machine Translated by Google

Der findes mange digitale identitetssystemer i verden i dag, der betjener forskellige naturlige netværk

De digitale identitetssystemer, der findes i dag, dækker en bred vifte af formål, omfang og sofistikering. Nogle systemer har et digitalt element boltet oven på det, der fundamentalt set stadig er et fysisk identitetssystem, mens andre er fuldt digitale og er bygget til at skalere og udvide sig i takt med at brugernes behov udvikler sig.

Forskellige identitetssystemer blev undersøgt, herunder systemer for alle brugergrupper, for at forstå landskabet af digitale identitetsløsninger, kategorisere disse systemer og drage konklusioner på overordnet niveau om, hvilke systemer der bedst passer til forskellige behov.

TYPER AF DIGITALE IDENTITETSSYSTEMER

Systemer til enkeltpersoner

Størstedelen af identitetssystemer er designet til enkeltpersoner og er ofte regeringsdrevne systemer.

Formål:

Designet til at øge økonomisk eller social inklusion og strømline leveringen af tjenester eller til at kontrollere adgangen til interne systemer for en enkelt organisation

Systemer for juridiske enheder

Identitetssystemer for juridiske enheder har ofte form af centraliserede informationsregistre, der ejes af en enkelt regering eller forsyningsvirksomhed.

Formål:

Har til formål at standardisere data på tværs af enheder, strømline processer og muliggøre dataaggregering på makroniveau

Systemer til aktiver

Identitetssystemer for aktiver tager ofte form af et centraliseret register eller et internt system for en enkelt organisation.

Formål:

Har til formål at præcisere ejerskab, standardisere data eller muliggøre driften af netværkssystemer

Machine Translated by Google

De mest betydningsfulde forskelle i identitetssystemer falder på tværs af tre primære dimensioner

Primære valgdimensioner er de valg, der skal træffes i designet af et digitalt identitetssystem, og som har størst indflydelse på systemets funktion og struktur.

Disse er ikke altid bevidste valg; de er ofte et naturligt resultat af den ramme, hvori systemet implementeres, og det problem, som systemet er beregnet til at løse, eller de behov, som det er beregnet til at imødekomme. De tre primære dimensioner af valg er:

Arten af identitetsbestemmelse

Er der én enkelt kilde til identitetsoplysninger? Er der et begrænset antal parter, der leverer attributter? Er identitetsleveringen fordelt på tværs af mange forskellige enheder?

Centraliseret:
Én enhed opbevarer og giver identitetsoplysningerne

Fødereret:
En begrænset antal enheder butik og give identitetsoplysninger

Distribueret:
Mange forskellige enheder opbevarer og give identitetsoplysninger

Antal afhængende parter

Er der én RP, der kan få adgang til brugerattributter, eller er der mange RP'er, der kan få adgang til brugeroplysninger?

En:
Systemet har én RP, der kan tilgå identitetsoplysninger

Mange:
Systemet indeholder mange RP'er, der har adgang til identitetsoplysninger

Informationsoverførslens art

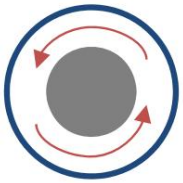
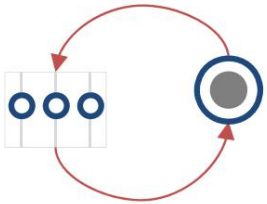
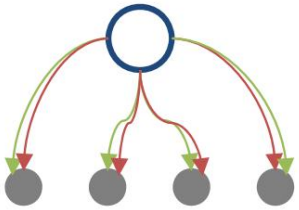
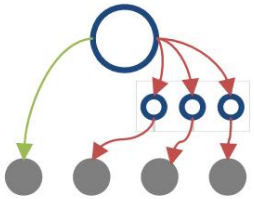
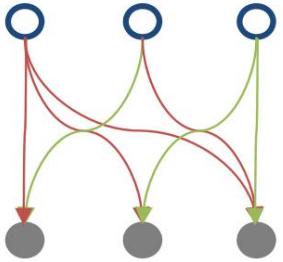
Overføres oplysninger fra IdP'en til RP'en med det formål at autentificere en bruger, eller overføres brugerattributter, som RP'en kræver for at udføre en given transaktion?

Godkendelse:
IdP'en autentificerer brugeren for RP'en, hvilket giver RP'en mulighed for at gennemføre transaktioner ved hjælp af oplysninger eller poster, som RP'en holder

Transaktion:
RP kræver oplysninger fra IdP med det formål at gennemføre en transaktion for bruger

Machine Translated by Google

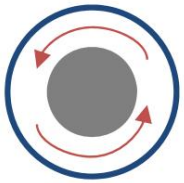
Vi har defineret fem forskellige arketyper, der udviser betydelige forskelle i struktur og formål.

	Intern identitetsstyring	Ekstern godkendelse	Centraliseret identitet	Federeret godkendelse	Distribueret identitet
Struktur	 Én enhed fungerer som både IdP og RP	 Mange IdP'er autentificerer brugere til en enkelt RP	 Én IdP betjener mange RP'er	 Et fast antal IdP'er godkende brugere til mange RP'er	 Mange IdP'er betjener mange forskellige RP'er
Informationsstrøm	• Systemet giver brugerne inden for et enkelt netværk adgang til tjenester, som de har tilladelse til at få adgang til baseret på deres attributter • Alle brugerattributter er opbevares inde i den enkelte enhed og bruges til at give brugerne tilladelse til enten at give eller nægte adgang til en given tjeneste eller sti	• Systemet godkender brugere til RP baseret på deres godkendelse til én af et sæt af IdP'er • Ingen attributter er overført mellem IdP'erne og RP'en; godkendelsestransaktionen bruges til blot at give eller nægte brugeren adgang til tjenester tilbudt af RP	• Systemet har en enkelt IdP, der autentificerer brugere og overfører eller eksponerer attributter til mange forskellige RP'er	• Systemet har en enkelt IdP, der lagrer brugeroplysninger, mens et separat sæt af IdP'er godkender brugere, der er forsøger at handle med RP'er • Efter godkendelse er de anmodede attributter overført fra IdP, der holder attributter til den RP, som brugeren handler med	• Systemet involverer flere IdP'er, der autentificerer brugere og overfører attributter til mange forskellige RP'er

Machine Translated by Google

Interne identitetsstyringsløsninger er designet til brug af én enhed

INTERN IDENTITETSHÅNDTERING



I interne identitetsstyringssystemer fungerer den samme enhed som en IdP og en RP. Enheden bruger oplysninger, den har om brugere, til at give dem adgang til forskellige interne tjenester.

Et godt eksempel på et internt identitetsstyringssystem ville være en virksomhed eller en regering, der giver sine medarbejdere eller borgere adgang til forskellige tjenester baseret på deres attributter.

NØGLEARKETYPEFUNKTIONER

- IdP/RP'en ejer de nødvendige attributter til at bestemme brugeren tilladelser i organisationen
- Systemet bruges til at kontrollere, hvilke brugere inden for en enkelt organisation eller enhed har tilladelse til at få adgang til bestemte tjenester
- Disse typer løsninger udvikles generelt af private organisationer og sælges som et produkt eller en tjenesteydelse til forskellige enheder og institutioner

CASESTUDIER

Lukkede interne styringssystemer *Private*

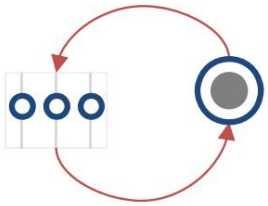
løsninger, globale førende

software som en løsning (SaaS)-udbydere som Salesforce, Oracle, SAP og Microsoft leverer løsninger, der hjælper deres kunder med bedre at forstå, administrere og interagere med en række brugere. SaaS er blevet en almindelig leveringsmodel for mange virksomheder, da disse løsninger hjælper med at holde brugere, data og applikationer sikre i et lukket system. Disse løsninger betjener en række forskellige brancher og brugergrupper (f.eks. kunder, medarbejdere, borgere osv.).

Machine Translated by Google

Eksterne autentificeringssystemer letter adgangen til tjenester med høj trafik

EKSTERN AUTENTIFIKATION



I eksterne godkendelsessystemer fungerer én enhed som både IdP og RP, men bruger et yderligere eksternt sæt af IdP'er til at godkende sine brugere. Formålet med dette system er at forbedre brugeroplevelsen for enkeltpersoner eller virksomheder, når de tilgår onlinetjenester; disse brugere kan bruge eksisterende logins i stedet for at vedligeholde flere brugernavne og adgangskoder for hver tjeneste.

NØGLEARKETYPEFUNKTIONER

- Systemet har én RP, ofte en regering, der opbevarer brugeroplysninger og udnytter et sæt etablerede institutioner som IdP'er (f.eks. finansielle institutioner, teleudbydere)
- IdP'erne er normalt betroede enheder, der udfører stærk autentificering i forbindelse med brugeronboarding, og de har derfor tillid til at yde et højt niveau af sikkerhed i forbindelse med identitetstransaktioner.
- Brugere kan bruge deres eksisterende godkendelsesmetoder via denne gruppe af IdP'er for at få adgang til RP'ens tjenester
- Både RP og IdP'er gemmer brugerattributter – godkendelsessystemet bruges til at verificere, at den enhed, der godkender via IdP'en, har tilladelse til at handle med RP'en.
- Ingen attributter overføres fra IdP'er til RP'en

CASESTUDIER

GOV.UK Verify

Offentlig-privat program, Storbritannien GOV.UK Verify-programmet er et eksternt godkendelsessystem, der giver britiske borgere adgang til offentlige tjenester online. Brugere bekræfter deres identitet online med en af ni IdP'er. Når brugerne er godkendt via en af disse udbydere, får de adgang til den offentlige tjeneste, de forsøger at få adgang til.

SecureKey Concierge

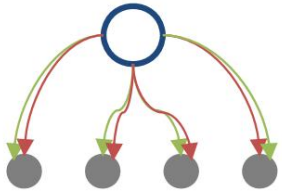
Offentlig-privat løsning, Canada

SecureKey Concierge er et digitalt godkendelsessystem, der giver enkeltpersoner mulighed for at vælge en betroet legitimationsoplysninger, de allerede har hos en af en række finansielle institutioner, for at få adgang til offentlige tjenester online. Brugerne logger ind med deres brugernavn og adgangskode til netbank og godkendes af deres bank. Når de er godkendt, får brugerne adgang til tjenesten. Ingen attributter overføres i systemet.

Machine Translated by Google

Centraliserede identitetssystemer bruger én IdP som en enkelt kilde til sandhed

CENTRALISERET IDENTITET



I centraliserede identitetssystemer fungerer en enkelt enhed som en IdP, der autentificerer brugere over for RP'er og overfører deres attributter. Disse systemer er ofte designet til at strømline servicelevering, muliggøre dataaggregering og give et enkelt overblik over brugere på tværs af flere RP'er.

NØGLEARKETYPEFUNKTIONER

- En enkelt IdP indeholder alle brugerattributter og ejer identitetssystemet; dette er ofte regeringen eller et andet centralt styrende organ
- IdP'en autentificerer brugeren til RP'en og overfører enten en fast eller en et skræddersyet sæt attributter til RP'en, der gør det muligt for den at gennemføre en transaktion på brugerens vegne
- Nogle systemer kræver, at RP'er betaler et gebyr for at bruge systemet og få adgang til brugerattributter
- Identitetsoplysninger kan overføres direkte via en fysisk formfaktor (f.eks. et smartkort) eller via et digitalt mæglersystem

CASESTUDIER

DigID-

regeringsprogram, Holland. DigID er et digitalt godkendelsessystem for hollandske statsborgere, der tilgår offentlige tjenester online. Individuelle attributter opbevares i et nationalt borgerregister; disse attributter bruges til at godkende brugere, når de ansøger om et DigID.

Enkeltpersoner kan derefter bruge deres DigID-brugernavn og adgangskode til at autentificere sig over for offentlige myndigheder. Deres nationale identifikationsnummer overføres fra det nationale borgerregister til RP.

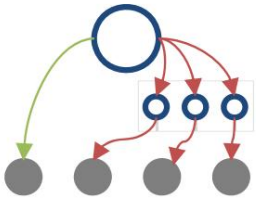
Folkeregisterets

regeringsprogram, Finland Folkeregisteret er en national database, der ejes og vedligeholdes af den finske regering. Regeringen fungerer som IdP og overfører attributter til offentlige og private RP'er. Formålet med systemet er at indsamle data, der kan bruges til valg, skatteindgivelse, retsadministration osv. Private RP'er kan også få adgang til disse data, hvis de betaler et gebyr og har fået brugerens samtykke.

Machine Translated by Google

Federerede godkendelsessystemer er afhængige af tredjeparter for at give brugeradgang til tjenester

FØDERERET AUTENTIKERING



I fødererede godkendelsessystemer bruger én IdP et sæt tredjeparter til at godkende brugere til en række RP'er.
Den primære IdP er den enhed, der lagrer og overfører brugerattributter. Disse systemer er designet til at forbedre login- og transaktionsprocesserne for brugere, der tilgår onlinetjenester, ved at give dem mulighed for at bruge et enkelt sæt legitimationsoplysninger til at godkende og overføre attributter til RP'er på deres vegne.

NØGLEARKETYPEFUNKTIONER

- Identitetsoplysninger opbevares centralt af én IdP
- Et sæt tredjeparts IdP'er fungerer som mæglere, der godkender brugere til RP'erne som de forsøger at handle med
- RP'er kan tilgå brugerattributter fra den primære IdP, ofte mod et gebyr; mange systemer kræver også udtrykkeligt brugersamtykke for at attributter kan overføres.
- I systemer, der tillader valgfri overførsel af attributter i stedet for et fast sæt af attributter, skal brugeren udtrykkeligt give samtykke til overførslen af specificerede attributter fra den primære IdP til RP'en.
- Disse systemer er ofte styret af regeringen, og regeringen fungerer som den centrale IdP, der opbevarer borger- eller enhedsdata

CASESTUDIER

NemID

Privat sektorløsning, Danmark NemID er

en elektronisk ID-, digital signatur- og sikker e-mailløsning, der giver enkeltpersoner adgang til offentlige og private tjenester. Regeringen udbudte systemet til den private sektor. Brugere bruger et fælles NemID-login og en fælles adgangskode samt unikke engangsadgangskoder til at autentificere sig til onlinetjenester. Brugerattributter gemmes i et centralt register.

Sverige BankID

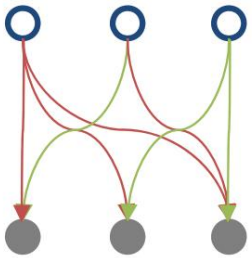
Offentlig-privat tjeneste, Sverige

Sverige har etableret et eID-system, der giver borgere og virksomheder adgang til over 300 offentlige og private tjenester. Digitale identiteter udstedes af en række private enheder, herunder store banker og en større telekommunikationsudbyder. Den offentlige sektor køber identitetsvalideringstjenester fra den private sektor.
Private tjenesteudbydere kan tilmelde sig BankID-systemet ved at underskrive kontrakter med eID-udbydere om godkendelse. Løsningen har været en stor succes; over 9 millioner borgere bruger i øjeblikket tjenesten.

Machine Translated by Google

Distribuerede identitetssystemer forbinder mange IdP'er og RP'er

DISTRIBUERET IDENTITET



I distribuerede identitetssystemer indsamler, lagrer og overfører mange IdP'er brugerattributter til mange RP'er. Disse systemer er bemærkelsesværdige ved, at de ikke er afhængige af attributter fra en enkelt IdP. Formålet med disse systemer er at give brugerne mulighed for nemt at interagere med mange forskellige enheder i et onlinemiljø ved at give dem en digital "wallet" af legitimationsoplysninger.

NØGLEARKETYPEFUNKTIONER

- Identitetsoplysninger kan lagres af flere IdP'er på en distribueret protokol (f.eks. blockchain), eller kan indsamles fra en række forskellige kilder og aggregeres af en enkelt enhed, der driver systemet
- Attributter kan overføres fra IdP'er til RP'er via en række forskellige metoder, herunder smartkort eller digitale/mobile protokoller
- Disse systemer er ofte privatejede og finansierede; regeringer eller andre offentlige organer spiller muligvis ikke en aktiv rolle i netværket
- Brugere ejer deres egne identiteter og kontrollerer ofte, hvilke transaktioner der finder sted og hvilke attributter overføres fra en eller flere IdP'er til RP'en
- Disse systemer har muligvis ikke et styringsorgan og er i stedet afhængige af fælles driftsstandarder for interoperabilitet

CASESTUDIER

TUPAS

Privat sektorløsning, Finland TUPAS er

et identitetssystem, hvor over 10 banker fungerer som IdP'er. Enkeltpersoner kan logge ind på en bred vifte af tjenester med legitimationsoplysninger fra deres bank. Brugernes fulde navne og nationale ID-numre overføres fra IdP'en til RP'en.

Global Legal Entity Identifier Foundation (GLEIF)

Den nonprofitorganisation, GLEIF,

støtter implementeringen af standarden for juridiske enheder (LEI). Dette system tildeler LEI'er til alle enheder, der interagerer med finansielle institutioner. Enheder kan bruge deres modparts LEI til at få adgang til deres identitetsoplysninger fra GLEIF's partnernetværk.

Mobilforbindelse

GSMA, global

Mobile Connect, er et digitalt identitetssystem, der autentificerer brugerne via deres enhed, hvilket giver brugerne adgang til en række forskellige tjenester. Dette eliminerer behovet for, at brugerne har mange brugernavne og adgangskoder for at få adgang til onlinetjenester.

Machine Translated by Google

Blockchain-teknologiens potentiale inden for identitet

Blockchain, eller distribueret ledgerteknologi (DLT), er en teknologiprotokol, der gør det muligt at dele data direkte mellem enheder i et netværk uden mellemled. DLT har visse nøglefunktioner, der rummer potentiale for identitetssystemer:

FUNKTIONER VED DISTRIBUTERET BOKS-TEKNOLOGI

Lave transaktionsomkostninger

Distribuerede ledgere eliminerer behovet for mellemled og sænker dermed omkostningerne ved at gennemføre transaktioner.

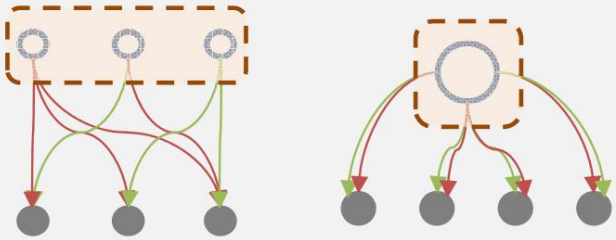
Uforanderlighed

Transaktionshistorikken vedligeholdes og verificeres via netværket, hvilket forhindrer forfalskning af oplysninger

Bekvemmelighed

Registerføring og transaktioner kan udføres fra enhver enhed, online eller offline

Illustrativt: Anvendelser af DLT i digital identitet



DLT har potentiale i identitetsapplikationer som en informationslagrings- og overførselsmekanisme inden for forskellige arketyper. DLT kan anvendes som en distribueret protokol, der giver brugerne mulighed for at gemme deres identitetsbekræftelser i en ledger og eksponere dem for forskellige RP'er, eller i et centraliseret system, hvor ledgeren ville ejes af en enkelt enhed, der ville give et samlet overblik over brugernes attestationer til brug i transaktioner, men ikke ville afsløre arten af legitimationsoplysningerne.

Der er i øjeblikket mange initiativer i gang, der undersøger det reelle potentiale for DLT i identitetssystemer; denne rapport vil ikke udforske dette emne i detaljer.

Machine Translated by Google

Den rigtige løsning til
Det rigtige problem

Machine Translated by Google

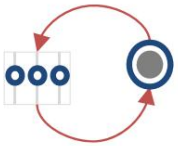
Arketyperne for digital identitet er bygget til at imødekomme meget forskellige behov

Intern identitetsstyring

Bedst egnet til: at administrere brugertilladelser i en enkelt enhed baseret på intern information for at sikre, at de rette personer har adgang til de rette ressourcer og slutpunkter. *Eksempel: Store organisationer, der har brug*

for en løsning til identitetsadgang og -administration for at kontrollere adgangen til deres interne tjenester med en udvalgt brugergruppe (f.eks. medarbejdere, kunder osv.).

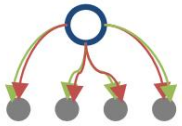
Ekstern godkendelse



Bedst egnet til: at strømline brugeradgang til en række tjenester, der tilbydes af én enkelt enhed, og eliminere proprietære logins

Eksempel: En regering tilbyder sine borgere onlinetjenester, der er kritiske, men sjældent brugte

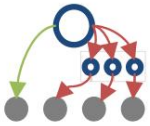
Centraliseret identitet



Bedst egnet til: at give en enkelt version af sandheden og et komplet, præcist og standardiseret overblik over ikke-fortrolige data på tværs af forskellige brugere

Eksempel: Et forsyningsselskab i branchen, der tilbyder et omfattende overblik over enhederne i den pågældende branche for at styre risiko og eksponering

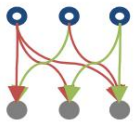
Federeret godkendelse



Bedst egnet til: at give en enkelt version af sandheden og et komplet, præcist og standardiseret overblik over data, samtidig med at brugerne kan autentificere sig over for en række tredjeparter, hvorved proprietære logins elimineres.

Eksempel: En regering muliggør identitetstransaktioner for sine borgere gennem samarbejde med tredjeparter

Distribueret identitet



Bedst egnet til: at integrere et stort antal IdP'er og RP'er, hvilket giver brugervenlighed, kontrol og privatliv i et onlinemiljø

Eksempel: En fuldt digital økonomi, der kræver flere uafhængige forbindelser mellem IdP'er og RP'er for at muliggøre brugertransaktioner.

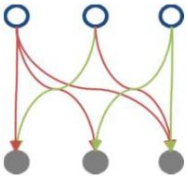
Machine Translated by Google

To af disse arketyper er velegnede til at løse brede identitetsproblemer

Centraliserede og distribuerede identitetssystemer er bedst egnede til at levere digital identitet i stor skala; disse to arketyper er dog ikke lige så velegnede til at levere identitet til forskellige brugergrupper.

FOR PERSONER

Distribueret identitet



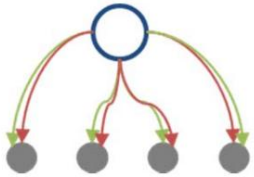
Distribuerede identitetssystemer er bedst egnede til at levere identitet til **enkeltpersoner** i stor skala • Distribuerede

identitetssystemer er bygget til at skalere til et stort antal IdP'er og RP'er, der muliggør et komplet sæt af bekvemme og effektive transaktioner for brugerne

• Disse systemer beskytter brugernes privatliv og øge kontrollen ved at give brugerne mulighed for at vælge, hvilke enheder der opbevarer deres oplysninger, og ved at fjerne et enkelt fejlpunkt fra systemet.

FOR JURIDISKE ENHEDER OG AKTIVER

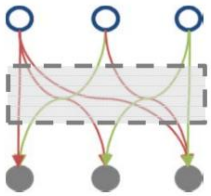
Centraliseret identitet



Centraliserede identitetssystemer er egnede til at levere identitet til **juridiske enheder** og **aktiver** i stor skala • Centraliserede

identitetssystemer tilbyder et konsolideret og standardiseret overblik over identitetsoplysninger og tilbyder den eneste kilde til sandhed, der kræves for transaktioner, der involverer juridiske enheder og aktiver, for at levere central værdi til eksterne interessenter såsom regulatorer.

Distribueret identitet



Distribuerede identitetssystemer er også velegnede til at levere identitet til **juridiske enheder** og **aktiver** i stor skala; disse identitetssystemer bør dog have en "wallet" eller et aggregeringslag, der kan give et samlet overblik over brugeren.

• Distribuerede identitetsløsninger tilbyder identitet i stor skala, og en Aggregeringslaget giver den samlede brugervisning, der kræves for juridiske enheder og aktiver

Machine Translated by Google

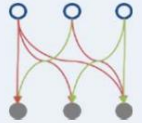
De centraliserede og distribuerede identitetsarketyper ville også løse mange af de forretningsmæssige udfordringer, som finansinstitutter i øjeblikket oplever.

I DETAILHANDEL / SMÅ OG MELLEMSTORE VIRKSOMHEDSBANKER

Behovet:

- Pålidelige, opdaterede individuelle identitetsoplysninger
- Mulighed for at få adgang til yderligere brugerattributter med samtykke
- Mulighed for internt at forbinde identitetsoplysninger for at give et samlet overblik over kunden
- Sikre lagre til brugeroplysninger for at forhindre identitetstyveri pga. stjålne data

Distribueret identitet



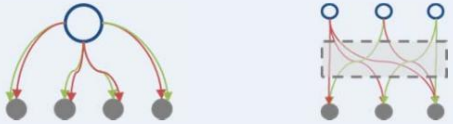
Distribueret identitet for enkeltpersoner ville give finansielle institutioner adgang til betroede brugeroplysninger og forbinde dem tilbage til en enkelt brugeridentitet; det ville også sikre, at brugeroplysninger opbevares sikkert med redundans i tilfælde af brud.

I ERHVERVS- OG INVESTERINGSBANKVERKSAMHED

Behovet:

- Pålidelige, opdaterede brugeridentitetsoplysninger
- Synlighed af oplysninger om aktiver og brugeridentitet
- Mulighed for at forbinde aktiv-, enheds- og individuelle oplysninger
- Mulighed for at aggregere identitetsoplysninger på tværs af enheder

Centraliseret identitet | **Distribueret identitet**



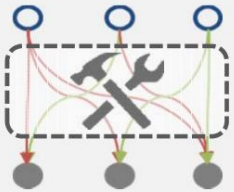
Centraliseret identitet og **distribueret identitet med et aggregeringslag** for juridiske enheder og aktiver ville give FI'er en konsolideret, pålidelig kilde til digitale attributter til disse brugere.

Machine Translated by Google

Konfiguration og implementering af et identitetssystem kræver mange yderligere valgmuligheder ud over arketypevalg.

Konfiguration af et identitetssystem kræver, at der træffes valg i forhold til et sekundært sæt af dimensioner, der ikke har den samme centrale funktionelle og strukturelle betydning som de primære dimensioner, men som har stor indflydelse på, hvordan systemet vil fungere. Valgene, der træffes i forhold til de sekundære dimensioner, bør derfor skræddersys til at passe til de specifikke behov og krav i det naturlige identitetsnetværk.

ILLUSTRATIV: SEKUNDÆRE VALGTE DIMENSIONER



Typer af IdP'er og RP'er: Hvilke typer enheder har tilladelse til at fungere som IdP'er og RP'er i identitetssystemet?

Mæglermekanisme: Hvordan er RP-forespørgsler forbundet med IdP-attesteringer? Kan systemet understøtte attributeksponering og attributforespørgselstransaktioner? Understøtter systemet transaktionsblinding?

Datahåndtering: Hvor gemmes data – i en central database, på et smartkort, på en distribueret protokol (f.eks. blockchain)? Aggregeres brugerattributter af en tredjepart?

Skalering: Er systemet designet til at skalere ud over dets oprindelige sæt af applikationer?

Forretningsmodel: Hvilken forretningsmodel understøtter systemet? Hvem finansierer systemet?

Styring: Hvem er ansvarlig for systemstyring og -tilsyn? Hvem er ansvarlig for systemdrift?

Brugerrettigheder: Hvilken grad af kontrol har brugerne over de oplysninger, der opbevares i systemet, hvem der opbevarer dem, og hvornår og hvordan de deles?

Bemærk: Dette er ikke en udtømmende liste over valgmuligheder; mange yderligere valg skal foretages

Det er umuligt at give en udtømmende liste over de sekundære dimensioner, der er valgfrie i konfigurationen og implementeringen af et identitetssystem, eller at give anbefalinger i forhold til hver enkelt. Der er derfor udviklet et sæt vejledende principper for at styre sekundær beslutningstagning og for at hjælpe med at levere et robust identitetssystem, der passer til interessenternes behov.

Machine Translated by Google

Vejledende principper

Machine Translated by Google

Et succesfuldt naturligt identitetsnetværk er et produkt af de valg, der træffes i forhold til de sekundære dimensioner. Fem principper informerer beslutningstagningen omkring disse valg og styrer udviklingen af robuste, værdiskabende systemer.

VEILEDENDE PRINCIPPER FOR DIGITAL IDENTITET

Socialt gode

Systemet er designet som et socialt gode, der er tilgængeligt for alle brugere og vil give maksimal gavn til en række interessenter.

Privatlivsfremmende

Brugeroplysninger eksponeres kun for de rigtige enheder under de rigtige omstændigheder

Brugercentreret

Brugere har kontrol over deres oplysninger og kan bestemme, hvem der opbevarer og får adgang til dem

Levedygtig og bæredygtig

Systemet er bæredygtigt som virksomhed og er modstandsdygtigt over for skiftende politiske prioriteter

Åben og fleksibel

Systemet er bygget på åbne standarder for at muliggøre skalering og udvikling; standarder og retningslinjer er transparente for interessenter.

Machine Translated by Google

Identitetssystemer bør give identitet til alle brugere, tjene brugerinteresser og være tilgængelige for alle enheder, der ønsker at foretage transaktioner i dem.

SOCIALT GODT

BAGGRUND

Evnen til at bevise identitet gør det muligt for brugere at blive integreret i formelle finansielle og sociale systemer og deltage i nødvendige og grundlæggende daglige transaktioner; digital identitet bør derfor betragtes som et socialt gode, som alle enheder bør have adgang til.

IMPLIKATIONER

• Systemet bør designes til at skaleres til alle brugere og netværksinteressenter, der ønsker det deltage

• Den offentlige sektor bør have en vis inddragelse i at definere systemets driftsprincipper parametre og regulatoriske standarder for at sikre, at brugernes interesser beskyttes, og for at øge systemets skala • Systemadgangsmekanismer

(f.eks. mobile platforme) bør demokratisere adgangen

IMPLIKATIONER FOR FI'ER

• Finansinstitutter har relationer med et stort antal brugere; denne skala kan fungere som katalysator for at fremme systemadoption og -optagelse •

Finansinstitutter spiller en nøglerolle i at sikre, at identitetssystemer er et værktøj til at øge den økonomiske inklusion

CASESTUDIER

SASSA

Offentlig-privat partnerskab, Sydafrika.

Det sydafrikanske socialsikringsagentur, Grindrod Bank og MasterCard har udstedt biometriske debetkort til over 22 millioner socialsikringsmodtagere.

SASSA-kortet indeholder en persons personlige oplysninger på chippen, autentificeres via biometri (fingeraftryk og stemmemønster) eller et personligt identifikationsnummer (PIN-kode) og er direkte knyttet til en bankkonto, hvor sociale tilskud indbetales.

Slutresultatet er, at over 5 millioner mennesker bliver økonomisk inkluderet, og at fordelingen af sociale tilskud i Sydafrika bliver enormt effektiviseret.

Machine Translated by Google

Identitetssystemer bør fremme privatlivets fred og beskytte brugeroplysninger mod ulovlig adgang, utilsigtet eksponering og overeksponering.

PRIVATLIVSFORBEDRING

BAGGRUND

Nuværende identitetssystemer sætter brugerne i fare og gør brugeroplysninger sårbare over for krænkelse af privatlivets fred, datalækage og overeksponering. Et digitalt identitetssystem bør beskytte brugeroplysninger og sikre, at kun det nødvendige afsløres for registrerede personer, og at disse parter kun bruger dataene til de oplyste formål.

IMPLIKATIONER

- Alle egenskaber, herunder demonstreret adfærd og præferencer, bør dækkes i en identitetssystem
- Attributoverførsel bør bruge nye informationsudvekslingsprotokoller, der tillader endpoint blændende
- Mæglermekanismen, der forbinder slutpunkterne for identitetsforespørgsler, bør kun tillade, at den minimalt krævede information for at fuldføre attributforespørgsel eller attributeksponeringstransaktioner eksponeres for RP'en.

- Attributter bør kun opbevares af IdP'er med tilstrækkelig datasikkerhed (som defineret af system standarder)
- Brugere eller depotansvarlige skal have indsigt i anmodede identitetstransaktioner og en defineret klagemetode, hvis deres oplysninger misbruges
- Opbevaring af følsomme oplysninger bør ikke være centraliseret for at reducere alvorligheden af konsekvenser og indvirkningen på brugerne i tilfælde af et databrud

IMPLIKATIONER FOR FI'ER

- Finansinstitutter bør opbygge cyberrobuste identitetssystemer og opfylde standarder fastsat af styringsorganet vedrørende databeskyttelse og -lagring
- Finansielle institutioner skal indhente brugersamtykke for at få adgang til eller dele attributter

CASESTUDIER

TUPAS

Privat identitetsløsning, Finland. I det finske TUPAS-system fungerer et sæt FI'er som IdP'er og overfører brugeroplysninger på deres vegne til RP'er. Brugeren har indsigt i, hvilke attributter RP'en anmoder om, og skal give samtykke til, at udvekslingen kan finde sted.

Kørekort

Offentlige løsninger, globale
Traditionelle kørekort er en almindeligt anvendt form for identitetsbevis. De kompromitterer dog privatlivets fred ved at tillade RP'en at læse alle brugerens oplysninger i stedet for kun de oplysninger, der kræves til transaktionen.

Machine Translated by Google

Identitetssystemer bør give brugerne kontrol over opbevaring og overførsel af deres personlige oplysninger

BRUGERCENTRISK

BAGGRUND

Mange identitetssystemer er fejlet på grund af manglende brugertilslutning, drevet af bekymringer omkring systemernes funktion og formål. Et vellykket digitalt identitetssystem, der tjener som et socialt gode, bør give brugeren (eller brugerens vogtere) kontrol over identitetsoplysninger.

IMPLIKATIONER

• Der bør tages hensyn til den gensidige identitet; brugere eller vogtere skal have klar indsigt om hvem der anmoder om deres oplysninger, og til hvilket formål •

Identitetstransaktioner bør kræve samtykke; undtagelser skal være klart definerede og meddelt, og brugerne bør underrettes om, hvornår deres oplysninger er blevet tilgået

• Brugere skal kunne tilbagekalde samtykke

• Brugere skal have kontrol over, hvor deres personlige oplysninger er gemt • Brugere skal nemt kunne opdatere deres oplysninger med IdP'er

IMPLIKATIONER FOR FI'ER

• Finansielle institutioner vil kunne anmode om identitetsoplysninger fra brugere for at skræddersy produkter og tjenester

• Finansinstitutter vil kræve brugersamtykke for at dele identitetsoplysninger

CASESTUDIER

ConsenSys

Privat løsning, USA I

ConsenSys-systemet kan brugerne uploade deres oplysninger og have fuld kontrol over, hvem deres data eksponeres for. Brugerne vælger ikke, hvem der gemmer deres data, fordi alle identitetsoplysninger gemmes på uPort – en brugerstyret applikation, der fungerer på blockchainen.

SecureKey Concierge

Offentlig-privat løsning, Canada

SecureKey Concierge-systemet giver canadiske borgere adgang til offentlige tjenester online ved at autentificere via et stort antal finansielle institutioner, som de allerede foretager transaktioner med.

Machine Translated by Google

Identitetssystemer bør designes som virksomheder, der er levedygtige og bæredygtige på lang sigt.

LEVETIDIG OG BÆREDYGTIG

BAGGRUND

Implementering af et digitalt identitetssystem er en betydelig indsats for alle interessenter; interessenter skal have sikkerhed for, at deres investering vil være umagen værd. Systemet skal derfor udformes som et levedygtigt og bæredygtigt projekt.

IMPLIKATIONER

• Den offentlige sektor bør spille en rolle i systemudvikling og implementering for at repræsentere brugernes interesser, fremme udbredelsen og sikre deltagelse fra myndighederne.

• Den private sektor bør involveres i systemudvikling og implementering for at sikre eksekveringsevne og operationel levedygtighed og sikre, at systemet er omkostningseffektivt. • Både den offentlige og den private sektor

bør spille en rolle i udviklingen af operationelle standarder.
inklusive:

– Ansvar og tvistbilæggelse
– Forretningsmodel
– Indsamling, lagring og overførsel af information
– Sikkerhedsniveauer
– Tekniske krav
– Modeller for brugersamtykke
– Revision

IMPLIKATIONER FOR FI'ER

• Finansinstitutter spiller en nøglerolle som vigtige og betroede private enheder i udformningen af systemets operationelle krav og standarder. • Finansinstitutter vil have

mulighed for at tjene penge på identitet som en tjeneste.

CASESTUDIER

Nationale ID-kort

Regeringsløsning, Storbritannien
Den britiske

regering indførte nationale ID-kort som et personligt identifikationsdokument. Systemet blev skrottet i januar 2010,

da den nye regering udtalte, at systemet var "spildfuldt, bureaukratisk og påtrængende" og udgjorde en betydelig trussel mod privatlivets fred og sikkerheden af personlige oplysninger.

Clarient Entity Hub, DTCC

Privat identitetsløsning, global Clarient

Entity Hub er et værktøj designet til at håndtere data og regulatorisk kompleksitet for parter, der deltager i finansielle transaktioner.

Det sigter mod at øge gennemsigtigheden på tværs af finansielle markeder og

tilbydes som en betalt tjeneste til andre enheder.

Machine Translated by Google

Identitetssystemer bør bygges på åben teknologi og datastandarder og bør designes til at integrere nye parter og imødekomme skiftende brugerbehov

ÅBEN OG FLEKSIBEL

BAGGRUND

Identitetssystemer, der er statiske og designet til et enkelt formål, er af natur begrænsede i omfang og har lav modstandsdygtighed over for miljøændringer. Et robust identitetssystem bør imødekomme skiftende krav og integrere nye parter.

IMPLIKATIONER

• Systemet skal bygges på åbne teknologistandarder • Systemet skal bygges på åbne datastandarder • Systemet skal have klare standarder omkring IdP'er og RP'er, således at nye enheder kan tilslutte sig system og overholde alle standarder og krav

• Systemet skal have et styringsorgan, der løbende tilpasser krav og standarder og overvåger systemets ydeevne

IMPLIKATIONER FOR FI'ER

• Åben teknologi og datastandarder vil mindske barrierer for brugere, der skifter institution

CASESTUDIER

X-Road

Offentlig løsning, Estland Det estiske digitale identitetssystem er bygget på en fælles teknologisk ramme kaldet X-Road. Denne ramme skaber interoperabilitet mellem forskellige databaser, hvilket øger det digitale identitetssystems funktionalitet og effektivitet betydeligt.

EU-lovgivning om e-identitet

Offentlig sektorløsning, EU-dækkende EU's e-identitetslovgivning sætter krav til medlemsstater, der udsteder identitet til borgere, for at sikre gensidig anerkendelse og omfanget af identitetssystemer i hele Europa.

Machine Translated by Google

De etablerede implikationer bør hjælpe med at vejlede beslutningstagningen omkring konfiguration af identitetssystemer

Det er vanskeligt at opbygge et succesfuldt identitetsnetværk. Der skal træffes en række valg for at sikre, at systemet leverer værdi til alle interessenter og vinder fremgang og accept. • De overvejelser på højeste

niveau i udviklingen af et identitetssystem er brugergruppen og det behov, som systemet skal tjene, og den arketypestruktur, der derfor bør overvejes. • Når disse overvejelser er afgjort, bør de sekundære dimensioner af valget ses i forhold til

de vejledende principper.

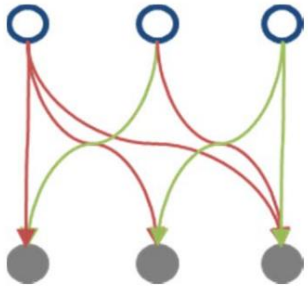
af digital identitet.

1
Problemer og brugergrupper

Den vigtigste overvejelse er brugergruppen og det problem, som identitetssystemet er designet til at løse; dette vil bestemme grænserne for det naturlige identitetsnetværk.

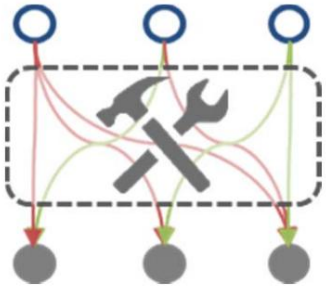
2
Valgfrie primære dimensioner

Brugergruppen og målproblemet vil styre valget af en passende identitetsarketype.



3
Valgfri sekundære dimensioner

De vejledende principper for identitet og deres implikationer vil hjælpe med at bestemme, hvilke strukturelle og konfigurationsmæssige valg der bør træffes i forhold til de sekundære dimensioner af valget.



Machine Translated by Google

Disse implikationer er meningsfulde for enheder inden for det digitale identitetsnetværk

Når interessenter konfigurerer identitetssystemer, skal de træffe en række beslutninger i hvert trin af processen.

ILLUSTRATIVT: Nogle åbne spørgsmål til identitetsinteressenter

1. Problemer og brugergrupper

- Hvilken brugergruppe betjener dette system? Hvilke problemer vil systemet løse? •
  Hvilke unikke karakteristika vil påvirke denne brugergruppes accept og brug af et identitetssystem? •
  Hvilken arketype er bedst egnet til at løse dette problem?

2. Valg af primære dimensioner

- Hvilke enheder bør fungere som IdP'er i dette
  system? • Hvilken type RP'er bør inkluderes i dette
  system? • Hvilken type information skal overføres i systemet?

3. Valgfri sekundære dimensioner

- Hvilken teknologistandard og tillidsramme vil systemet bruge? • Hvilken
  sikkerhedsmodel vil systemet bruge? • Skal
  systemet bruge en forretningsmodel baseret på identitet som en service og et gebyr for
  transaktioner? • Hvordan vil styringsorganet organiseres? Hvilke enheder vil være involveret i systemstyring?
- Hvordan vil brugeren give samtykke i transaktioner?
- Vil der blive tilladt undtagelser fra kravene til brugersamtykke? •
  Hvordan vil den offentlige sektor blive involveret i udformningen af de operationelle standarder?

Machine Translated by Google

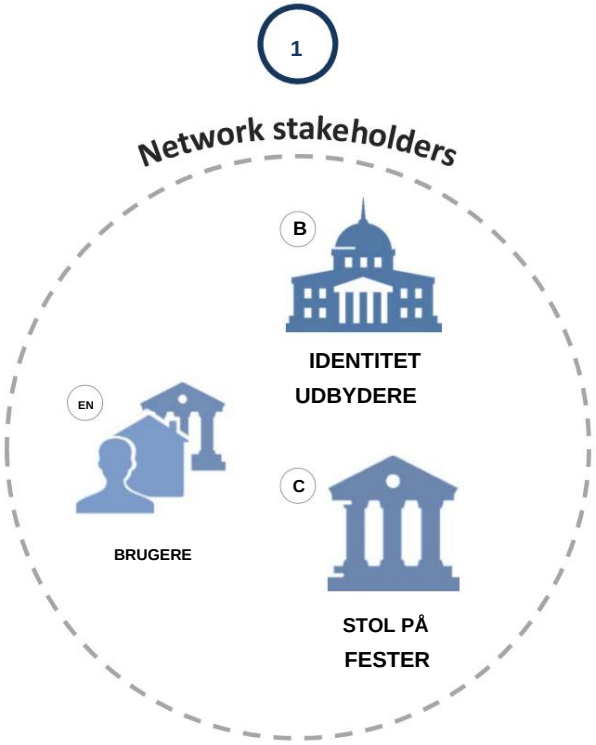
Fordele

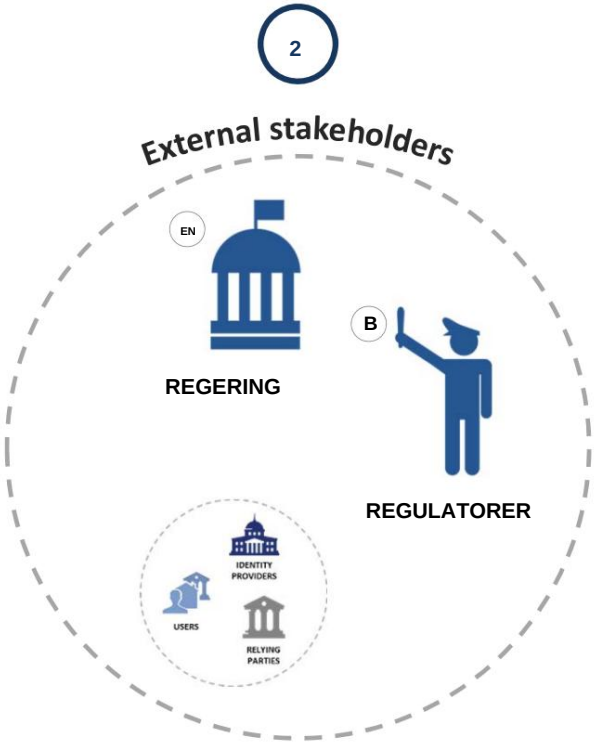
Machine Translated by Google

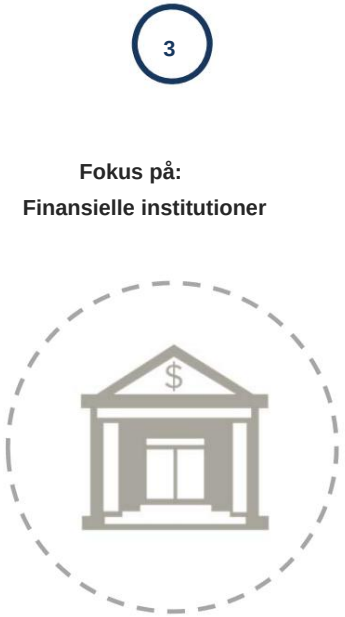
Implementeringen af digitale identitetsnetværk ville gavne en række forskellige interessentgrupper.

Identitetssystemer, der er konstrueret baseret på denne vejledning, vil give fordele både for de interessenter, der er direkte involveret i identitetsnetværket, og for eksterne interessenter. Især finansielle institutioner vil opnå store fordele som følge af implementeringen af digital identitet.

INTERESSENTGRUPPER







Machine Translated by Google

Hvilke fordele ville netværkets interessenter opnå?

Netværksinteressenter er parter, der er involveret i selve netværkets kernedrift. Netværksinteressenterne er brugere, IdP'er og RP'er.

EN

BRUGERE

Privatliv og kontrol

Brugere er i stand til at kontrollere hvem har adgang til deres attributter

Sikkerhed

Brugerattributter opbevares på trygge og sikre steder

Bekvemmelighed

Digital attributoverførsel giver brugerne mulighed for at handle effektivt

Gennemsigtighed

Brugere har indsigt i, hvordan og hvornår deres attributter vises

B

IDENTITET UDBYDERE

Omsætningsvækst

IdP'er kan opkræve gebyrer for behandling af identitetstransaktioner

Nedsat risiko og ansvar

IdP'er forstår deres ansvar i tilfælde af datatab eller brud

Konkurrencepræget positionering

IdP'er kan skabe et stærkt forhold til brugerne og positionere sig selv som en afgørende del af den digitale økonomi.

Forbedrede produkter og tjenester

IdP'er kan bruge detaljerede og betroet kunde information til at levere skræddersyede tjenester

C

STOL PÅ FESTER

Informationsnøjagtighed

RP'er har adgang til pålidelige, verificerede identitetsoplysninger

Færre transaktionsafbrydelser

En strømlinet bruger erfaring fjerner barrierer for at gennemføre transaktioner

Serviceskræddersyet

RP'er kan tilbyde mere skræddersyede produkter og tjenester

Mindsket risiko og ansvar

RP'er forstår deres ansvar i tilfælde af datatab eller brud

Serviceudbud

RP'er kan skelne mellem ulovlige og legitime brugere

Machine Translated by Google

Hvilke fordele ville brugerne opnå?

BRUGERE

Privatliv og kontrol

1. Privatliv og kontrol •

Brugere ville have fuld kontrol over, hvilke IdP'er der opbevarer deres attributter • Brugernes samtykke ville være påkrævet, før IdP'er kunne eksponere attributter til RP'er • Brugerdata ville ikke blive solgt af tredjeparter • Den minimale mængde brugerinformation, der kræves, ville blive overført under transaktioner

Sikkerhed

2. Sikkerhed •

Brugerattributter vil kun blive opbevaret af enheder, der opfylder systemstandarder og krav til informationshåndtering. og opbevaring

• Digital attributlagring ville gøre identitetsoplysninger modstandsdygtige over for beskadigelse, ødelæggelse eller tab • Brugere ville have mulighed for at sprede deres identitetsoplysninger, hvilket skaber en beredskabsplan, hvis en identitetsleverandør ville blive udsat for en dataansvarlig brud eller data blev slettet eller stjålet, og reduktion af virkningen af et databrud på brugeren

Bekvemmelighed

3. Bekvemmelighed

• Digital identitet og overførsel af digitale attributter ville forenkle og forbedre brugeroplevelsen i transaktioner, eliminerer behovet for, at brugerne skal spore flere godkendelsesmetoder (f.eks. brugernavne og adgangskoder) og manuelt indsende personlige oplysninger under transaktioner • Attributter overføres digitalt, hvilket fjerner risikoen for menneskelige fejl og efterfølgende information afhjælpning

• Brugere ville nemt kunne opdatere oplysninger, der opbevares hos deres IdP'er, og ville ikke skulle håndtere transaktioner udføres på baggrund af ukorrekte eller forældede oplysninger

Gennemsigtighed

4. Gennemsigtighed

• Brugere ville have indsigt i, hvilke attributter der ville blive eksponeret for, og til hvilken enhed under identitetstransaktioner

Machine Translated by Google

Hvilke fordele ville brugerne opnå?

BRUGERE: Casestudie

Estlands e-forvaltningssystem beskytter borgeroplysninger, giver brugerne en yderst bekvem oplevelse og giver dem mulighed for at føle ejerskab over deres data.

E-forvaltning

Offentlig løsning, Estland • Estlands

regering har skabt en digital grænseflade mellem borgere og offentlige myndigheder. Regeringen opbevarer borgeroplysninger i et centraliseret folkeregister og fungerer som IdP og styrende organ, der overfører pålidelige og troværdige data til RP'er.

• Borgerne får hver især tildelt et eID-identifikator, som de kan bruge til at logge på statsportalen, som giver adgang til snesevis af tjenester, lige fra afstemning til opdatering af bilregistre og ansøgning til universiteter. Regeringen overfører de attributoplysninger, der er nødvendige for at gennemføre hver transaktion, fra folkeregistret til RP, og borgerne kan se, hvilke enheder der har tilgået deres oplysninger.

• Borgere i Estland har mulighed for at se, hvem der har tilgået deres registre, hvor ofte og til hvilket formål. Denne gennemsigtighed giver borgerne mulighed for at føle ejerskab over deres data, da de kan se, hvordan oplysningerne bruges.

• Et overbevisende eksempel er den elektroniske patientjournal – et landsdækkende system, der integrerer data fra forskellige sundhedsudbydere i én portal. Brugere kan logge på en patientportal for at kontrollere deres behandling og administrere deres sundhedsoplysninger.

Chekk giver brugerne mulighed for at eje, administrere og dele deres personlige oplysninger

Tjek

Løsning til den private sektor, Global •

Chekk er en mobil løsning, der giver brugerne en sikker pung med deres personlige egenskaber og giver dem mulighed for at dele opdaterede oplysninger med de enheder, de handler med.

• I Chekk-systemet leveres kun de oplysninger, der kræves til en transaktion, hvilket betyder, at brugeren har kontrol, og deres privatliv er beskyttet beskyttet.

Machine Translated by Google

Hvilke fordele ville IdP'er opnå?

IDENTITETSUDBYDERE

Omsætning vækst

1. Omsætningsvækst

• IdP'er ville gennemføre identitetstransaktioner for RP'er; dette ville give dem mulighed for at tjene penge på identitet som en tjeneste gennem gebyrer pr. transaktion eller andre forretningsmodeller

Defineret risiko og ansvar

2. Defineret risiko og ansvar •

Retningslinjer for ansvar ville være klart defineret og kommunikeret; IdP'er ville være klare over deres ansvar i tilfælde af datatab eller -brud eller overtrædelse af standarderne for identitetsbestemmelse

Konkurrencepræget positionering

3. Konkurrencepræget positionering • IdP'er ville være i stand til at skabe et stærkt forhold til brugerne og positionere sig som en kritisk del af den digitale økonomi, givet deres unikke indsigt i brugerne og deres etablerede tillidsposition.

Forbedrede produkter og tjenester

4. Forbedrede produkter og tjenester •

IdP'er ville have øget adgang til detaljerede og pålidelige brugeroplysninger, der ville give dem mulighed for bedre at skræddersy processer, produkter og tjenester

• IdP'er kunne begynde at trække på ikke-standardiserede brugerattributter for bedre at kunne håndtere og evaluere risici (f.eks. patientjournaler). • Sikre digitale identitetsprotokoller og overførsel af digitale attributter ville forbedre brugeroplevelsen og udvide antallet af af tjenester, som IdP'er sikkert kunne levere online

Machine Translated by Google

Hvilke fordele ville IdP'er opnå?

IDENTITETSUDBYDERE: Casestudie

En række banker fungerer som IdP'er i TUPAS-systemet og giver enkeltpersoner adgang til over 180 offentlige og private tjenester.

TUPAS

Løsning til privat sektor, Finland •

Federation of Finland Financial Services stod bag oprettelsen af et bankidentitetssystem kaldet TUPAS, der er designet til at forbedre brugervenligheden adgang til onlinetjenester.

• RP'erne betaler for tjenesten (opstartsgebyrer, månedlige gebyrer og gebyrer for fastsatte transaktionsvolumener). Brugere kan også blive opkrævet månedligt, afhængigt af deres forhold til deres bank. • Mens en gruppe teleselskaber i

Finland tilbyder en konkurrerende tjeneste, blev 95 % af alle online-tjenestelogin pr. februar 2016 behandlet via TUPAS. Kun 2 % af online-tjenesteloginene blev behandlet via det konkurrerende system. Dette kan skyldes regeringens stærke adoption af TUPAS, borgernes loyalitet over for regeringen og bankerne eller det faktum, at det var den første succesfulde tjeneste i regionen. TUPAS har etableret en ny indtægtskilde for banker samt en stærk konkurrencemæssig position.

• Hos de fleste banker skal brugeren godkende og bekræfte, at de data, der overføres fra banken til RP'en, er nøjagtige, hvilket eliminerer enhver ansvarsrisiko for IdP'en.

Machine Translated by Google

Hvilke fordele ville RP'er have?

FORLIDENDE PARTER

Information nøjagtighed

1. Informationsnøjagtighed •
Repræsentanternes ansvarspersoner ville have adgang til pålidelige, verificerede identitetsoplysninger, der matcher det sikkerhedsniveau, der kræves for deres produkter eller tjenester; dette ville eliminere behovet for informationssanering og krydstjek af oplysninger via betalte tredjepartstjenester.

• Digital attributudveksling ville eliminere risikoen for menneskelige fejl i transaktioner

Serviceskræddersyet

2. Tilpasning af tjenester • RP'er vil være i stand til at levere mere skræddersyede produkter og tjenester til brugere ved at anmode om adgang til identitet oplysninger ud over, hvad de traditionelt ville have brug for til at gennemføre transaktioner

Serviceudbud

3. Tjenestelevering •
Mere pålidelige og præcise identitetsprotokoller ville give RP'er større mulighed for at skelne mellem ulovlige og legitime brugere, og at nægte eller levere tjenester i overensstemmelse hermed

Nedsat transaktionsopgivelse

4. Færre transaktioner, der afbrydes • En mere strømlinet brugeroplevelse ville fjerne barrierer for at gennemføre transaktioner (f.eks. glemt login oplysninger, påkrævet kontooprettelse, afviste faktureringsoplysninger) og ville derfor reducere antallet af brugeres afbrydelser af transaktioner

Nedsat risiko og ansvar

5. Mindsket risiko og ansvar •
Retningslinjer for ansvar ville være klart definerede og kommunikerede; ansvarlige personer ville være klare over deres ansvar i tilfælde af af datatab eller brud eller overtrædelse af standarderne for identitetsbestemmelse

Machine Translated by Google

Hvilke fordele ville RP'er have?

FORLIDENDE PARTER: Casestudie

Folkeregistret er en central database, der lagrer identitetsoplysninger – dataene er betroede af mange enheder i Finland som en omfattende kilde til opdaterede oplysninger om borgere, aktiver og juridiske enheder.

Folkeregisterets

regeringsprogram, Finland • Folkeregisteret

er en national database, der ejes og vedligeholdes af den finske regering. Regeringen fungerer som IdP,
overførsel af attributter til offentlige og private RP'er.

- Borgere er forpligtet til at give opdaterede oplysninger til folkeregistret, således at IdP'er kan have tillid til, at de oplysninger, de modtager er præcise.
- Offentlige RP'er, der kræver attributter for at gennemføre transaktioner, kan bruge borgernes nationale ID-numre til at få adgang til data, der opbevares i Folkeregister. De nødvendige attributter overføres digitalt fra registeret til personnummeret.
- Private personelle ansvarspersoner kan også abonnere på folkeregisteret og få adgang til oplysninger (med samtykke) for at levere bedre produkter og tjenester til deres brugere.

Machine Translated by Google

Hvilke fordele ville der være for eksterne interessenter?

Eksterne interessenter er parter, der ikke er involveret i systemets daglige drift, men som er centrale interessenter i systemet. De eksterne interessenter er regeringer og regulatorer.

EN

REGERINGER

Processtrømning og effektivisering

Myndighederne kan interagere mere effektivt med deres borgere og dermed spare tid og penge

Forbedret servicelevering

Myndighederne kan lettere identificere og levere tjenester til forskellige grupper af borgere

B

REGULATORER

Sporing af aktiver

Tilsynsmyndigheder kan mere effektivt spore aktivers oprindelse og ejerskab

Gennemsigtig visning af enheder

Tilsynsmyndigheder kan få adgang til en samlet visning af juridiske enheder på tværs af deres hierarkier

Forbedret overholdelse

Regulatorer kan få adgang til pålidelige, opdaterede attributoplysninger for brugere, hvilket forbedrer effektiviteten af den samlede compliance-proces.

Datastandardisering

Dataindsamling og -lagring kan standardiseres på tværs af alle FI'er, hvilket reducerer friktion i dataaggregering

Machine Translated by Google

Hvilke fordele ville regeringerne opnå?

REGERINGER

Behandle strømlining og effektivisering

1. Processtrønling og effektivisering •

Myndighederne ville være i stand til at interagere mere effektivt med deres borgere og dermed spare tid og penge i forbindelse med levering af tjenester såsom selvangivelse og uddeling af socialhjælp

Forbedret service levering

2. Forbedret servicelevering •

Myndighederne ville være i stand til at udnytte præcise identitetsoplysninger til lettere at identificere enkeltpersoner og enheder, der er berettigede til at få adgang til givne tjenester

• Regeringer ville nemt kunne identificere og levere tjenester til dem, der kan være økonomisk eller socialt vanskelige udelukket på grund af manglende traditionelle identitetsoplysninger

Machine Translated by Google

Hvilke fordele ville regeringerne opnå?

REGERINGER: Casestudie

Aadhaar-programmet blev introduceret i Indien for at øge social og økonomisk inklusion ved at give identitet til alle indiske indbyggere, hvoraf mange tidligere ikke havde nogen mulighed for at bevise deres identitet.

Aadhaar

Regeringsprogram, Indien • Aadhaar-

kortet blev udviklet for at forbedre økonomisk inklusion i landet. Den unikke identifikationsmyndighed i Indien (UIDAI) fungerer som den centrale IdP og kontrollerer, hvem der har adgang til de data, de indsamler og opbevarer.

• For at modtage et kort skal enkeltpersoner indsende forskellige dokumenter til en lokal registrator. Hvis de ikke kan fremvise dokumentation, skal en "Introducerende personer", såsom en valgt repræsentant eller en lokal lærer eller læge, kan bekræfte personens identitet. Denne parallelle proces mindsker risikoen for, at UIDAI opbevarer unøjagtige oplysninger eller yder sociale tjenester til illegale indvandrere eller andre ulovlige aktører.
UIDAI har en database, der indeholder oplysninger såsom navn, fødselsdato og biometriske data, der kan omfatte et fotografi, fingeraftryk, iris-scanning eller andre oplysninger.

• Aadhaar-programmet har været meget effektivt til at øge den økonomiske inklusion med over 1 milliard mennesker tilmeldt konti, men der er stadig nogle udestående bekymringer om informationsbeskyttelse og privatliv.

Det estiske e-opholdsprogram giver ikke-estiske statsborgere mulighed for at få digital opholdstilladelse i landet.

E-residens

Regeringsprogram, Estland • E-

opholdsprogrammet giver ikke-estiske statsborgere mulighed for at få et digitalt ID-kort, der gør det muligt for dem at bruge estiske private og offentlige tjenester tjenester og at bruge sikre digitale signaturer. Formålet med programmet er at skabe et virtuelt forretningsmiljø og fortsat positionere Estland som et knudepunkt i den digitale verden

• Siden starten i december 2014 har næsten 10.000 personer ansøgt om e-residency, og over 400 har etableret en ny virksomhed med hjemsted i Estland.

Machine Translated by Google

Hvilke fordele ville der være for regulatorer?

REGULATORER

Sporing af aktiver

1. Sporing af aktiver •

Tilsynsmyndighederne ville være i stand til mere effektivt at spore aktivernes oprindelse og ejerskab, hvilket ville øge deres evne til at spore udbyttet af kriminel aktivitet.

• Genpantsættelse af aktiver kunne spores, hvilket sikrede, at aktiver ikke ville blive genpantsat ud over deres samlede værdi

Gennemsigtig visning af enheder

2. Gennemsigtigt overblik over enheder

• Tilsynsmyndigheder ville have adgang til et samlet overblik over juridiske enheder på tværs af deres hierarkier, hvilket øger deres evne til at evaluere systemisk risiko og styre stabilitet

Forbedret overholdelse

3. Forbedret compliance •

Adgang til pålidelige identitetsoplysninger ville øge FI'ers evne til at overholde reglerne for bekæmpelse af hvidvaskning af penge. Kend din kunde og andre regler inden for deres jurisdiktion

• Adgang til pålidelige oplysninger om juridiske enheder og aktividentitet ville give finansielle institutioner mulighed for mere præcist at opdage penge hvidvaskning og andre mistænkelige transaktioner

• Adgang til betroede digitale attributter ville give FI'er mulighed for at automatisere deres compliance-processer i et vist omfang potentielt give tilsynsmyndighederne mulighed for at øge den krævede hyppighed af compliance-evalueringer

Datastandardisering

4. Datastandardisering •

Dataindsamling og -lagring kan standardiseres på tværs af alle finansielle institutioner, hvilket reducerer friktionen i dataaggregering

Machine Translated by Google

Hvilke fordele ville der være for regulatorer?

REGULATORER: Casestudie

GLEIF er en organisation, der støtter implementeringen af Legal Entity Identifier-standarden – denne standard kan i sidste ende blive en rød tråd mellem identifikationssystemer i et forsøg på at skabe et standardiseret globalt overblik over juridiske enheder.

Global Legal Entity Identifier Foundation (GLEIF)

Nonprofitorganisation, global • GLEIF

administrerer et netværk af lokale driftsenheder, der udsteder juridiske enhedsidentifikatorer (LEI'er) til juridiske enheder verden over. • Juridiske enheder,

der deltager i finansielle transaktioner, indsender et standardsæt af attributter til en lokal driftsenhed, som validerer dem mod tredjepartsregistre og derefter udsteder en LEI. GLEIF opbevarer masterfilen over alle LEI'er og tilhørende enhedsoplysninger. • Systemet blev introduceret af finansielle tilsynsmyndigheder for at

forbedre mikro- og makroprudentiel risikovurdering og -styring.

øge markedets gennemsigtighed og forbedre nøjagtigheden af finansielle data.

- Ud over finansielle tjenester og regulering er målet med LEI-systemet at levere pålidelige identitetsoplysninger, der muliggør unikke identifikation af juridiske enheder verden over, inden for finansielle tjenesteydelser og andre steder (f.eks. forsyningskædeapplikationer).
- Over 430.000 LEI'er er blevet udstedt siden oktober 2015. LEI'en er beregnet til at blive forbindelsen mellem alle andre identifikationssystemer (f.eks. kend-din-kunde-systemer, virksomhedsregisterkoder osv.). Dette vil give tilsynsmyndighederne et ensartet og omfattende overblik over alle juridiske enheder og finansielle instrumenter globalt.

Machine Translated by Google

Finansielle institutionelle institutter har unikke fordele, der gør dem velegnede til at spille nøgleroller i digitale identitetsnetværk.

FORDELE VED FI'ER INDEN FOR DIGITAL IDENTITET

Finansielle institutioner er meget afhængige af identitet

Identitet er central for FI'ernes funktion, mens de bærer en stor del af omkostningerne ved ineffektive identitetsprotokoller.

Finansielle institutioner er forbundet med mange vigtige identitetsinteressenter

Finansinstitutter har etablerede relationer med brugere, regeringer, tilsynsmyndigheder og andre vigtige interessenter og har erfaring med at arbejde med disse grupper om centrale problemstillinger, samtidig med at de afvejer konkurrerende interesser.

Finansinstitutter er betroede institutioner

Forbrugerne har større tillid til, at finansinstitutter opbevarer personlige oplysninger end andre institutioner, såsom regeringer, telekommunikations- og teknologivirksomheder.

Finansinstitutter har eksisterende forretningsmodeller, der ikke kræver direkte monetisering af kundeoplysninger

CASESTUDIER

iDIN

Privat sektorløsning, Holland iDIN blev skabt for at kapitalisere på de store investeringer, som banker har foretaget i onboarding af deres kunder; banker indsamler allerede yderst pålidelige identitetsoplysninger og er godt positioneret til at overføre dem til andre parter.

NemID

Privat sektorløsning, Danmark. For at maksimere udbredelsen af NemID ønskede bestyrelsen at samarbejde med private aktører, der ofte har brugt tjenesterne; banker interagerer ikke kun regelmæssigt med enkeltpersoner, men ses også som betroede institutioner, der allerede lagrer brugeridentitet.

SecureKey Concierge *Offentlig-privat program, Canada* SecureKey har indgået et partnerskab med ni banker, der er betroede og opbevarer nøjagtige data. Disse data kan bruges til at godkende enkeltpersoner i systemet.

Machine Translated by Google

Hvilke fordele ville implementeringen af digital identitet give finansinstitutter?

Fordelene for FI'er ved at implementere digital identitet falder i seks kategorier:

FINANSIEL INSTITUTIONER

Forbedrede produkter og tjenester

Finansinstitutter vil være i stand til at bruge detaljerede og pålidelige kundeoplysninger til at levere skræddersyede tjenester til kunderne.

Operationel effektivitet

Digital overførsel og håndtering af attributter vil give FI'er mulighed for at strømline og automatisere mange processer og dermed eliminere menneskelige fejl

Mindre svindel

Sikker, digital lagring af brugeroplysninger vil reducere svindel som følge af stjålne oplysninger eller kompromitteret godkendelse

Forbedret overholdelse

Digital attributhåndtering og bedre adgang til brugeridentitet vil gøre det muligt for FI'er at gennemføre compliance-processer lettere og mere præcist

Omsætningsvækst

Finansinstitutter vil have mulighed for at øge omsætningen fra forbedrede produkter og tjenester samt at tilbyde identitet som en tjeneste.

Bedre brugeroplevelse og konkurrencedygtig positionering

Finansinstitutter kan tilbyde en strømlinet brugeroplevelse og positionere sig som en kritisk del af det digitale økonomi

Machine Translated by Google

Hvilke fordele ville implementeringen af digital identitet give finansinstitutter?

FINANSIELLE INSTITUTIONER

Forbedrede produkter og tjenester

1. Forbedrede produkter og tjenester •

Finansinstitutter ville have øget adgang til detaljerede og pålidelige brugeroplysninger, der ville give dem mulighed for bedre at skræddersy processer, produkter og tjenester såsom:

- – Risikovurdering for forsikringsprodukter
- – Finansiel rådgivning
- – Formueforvaltning
- – Kreditvurdering
- – Lånetildeling

• Finansielle institutioner kunne begynde at trække på pålidelige oplysninger, med samtykke, for bedre at styre og evaluere risici; sikre digitale identitetsprotokoller og overførsel af digitale attributter ville forbedre brugeroplevelsen og udvide antallet af tjenester, som finansielle institutioner sikkert kunne levere online.

Operationel effektivitet

2. Operationel effektivitet •

Finansielle institutioner vil kunne tilgå brugeroplysninger i en konsolideret, digital form via forespørgsler i den digitale identitet netværk; at have attributter i en konsolideret digital form ville give et enkelt overblik over kunden og give FI'er mulighed for at strømline kundevendte operationer, såsom onboarding, samt mange backend-processer

• Digital identitet for aktiver vil give FI'er mulighed for at spore finansielle produkter og aktiver tættere gennem større synlighed ejerskab og løsning af bekymringer om genpantsættelse

Mindre svindel

3. Mindre svindel •

Brugeroplysninger ville kun blive opbevaret af enheder, der følger standarder for databeskyttelse; dette ville reducere svindel (såsom transaktioner med manglende kortvisning foretaget ved hjælp af forsendelses- og faktureringsoplysninger stjålet i forbindelse med store databrud)

• Digitale godkendelsesmetoder ville reducere svindel som følge af hackede eller kompromitterede brugerkonti

Machine Translated by Google

Hvilke fordele ville implementeringen af digital identitet give finansinstitutter?

FINANSIELLE INSTITUTIONER

Forbedret overholdelse

4. Forbedret compliance •

Digital identitet ville give FI'er adgang til pålidelige, opdaterede attributoplysninger for brugerne, hvilket forbedrer nøjagtigheden af Kend dine kunders processer

• Digital informationsoverførsel og -lagring vil give FI'er mulighed for at gennemføre deres compliance-processer hurtigere og nemmere, hvilket muliggør hurtigere behandling og reducerer den tid, der bruges på informationsafhjælpning og korrektion af menneskelige fejl.

• Compliance-processer kunne automatiseres og udføres med mere regelmæssige cyklusser • Digital identitet ville give FI'er bedre indsigt i virksomheders ejerstrukturer og identiteten af virksomheder direktører for at forbedre virksomhedens kendskabsprocesser til kunderne

• Digital identitet ville give FI'er bedre indsigt i aktivernes oprindelse og ejerskab

Omsætningsvækst

5. Omsætningsvækst •

Finansielle institutioner kan tjene penge på identitet som en tjeneste gennem forretningsmodeller såsom abonnementsgebyrer hos RP'er eller gebyrbaserede transaktionstjenester til identitetstransaktioner med høj sikkerhed, herunder:

– Godkendelse –

Digitale signaturer –

Fuldførelse af identitetstransaktioner for RP'er, såsom at angive attributoplysninger (f.eks. at angive forsendelsesoplysninger til forhandlere) eller at angive oplysninger om attributter (f.eks. at bekræfte over for en forhandler, at en bruger er over en bestemt alder baseret på fødselsdato)

Bedre bruger erfaring og konkurrencedygtig positionering

6. Bedre brugeroplevelse og konkurrencedygtig positionering • Ved at samarbejde med regeringer, offentlige enheder og andre private enheder vil FI'er blive en del af en et pålideligt økosystem, der arbejder på at udvikle den digitale økonomi

• Som betroede beskyttelsesorganer for brugeroplysninger ville finansielle institutioner styrke deres relationer med brugerne

Machine Translated by Google

Hvilke fordele ville implementeringen af digital identitet give finansinstitutter?

FINANSIELLE INSTITUTIONER: Casestudier

Aire kan hjælpe personer, der mangler traditionelle kreditoplysninger, ved at bruge ikke-traditionelle brugerattributter til at opbygge en ny kreditvurdering. score.

Aire

Den private virksomhed Aire, en britisk

startup, tilbyder et alternativ til traditionelle kreditvurderingsteknikker. Aire giver enkeltpersoner mulighed for at indsende en bred vifte af materialer, der bruges til at vurdere individets kreditværdighed; for eksempel kan en bruger indsende regninger fra forsyningsselskaber eller Netflix.

"Know-your-customer"-værktøjer giver FI'er adgang til pålidelige og opdaterede attributoplysninger for brugerne, hvilket forbedrer nøjagtigheden af individuelle og virksomhedsmæssige "know-your-customer"-processer.

Private løsninger, globale branchekendskabsværktøjer

til kunder, såsom Thomson

Reuters' OrgID eller DTCC's Clarient Entity Hub, er beregnet til at fungere som pålidelige lagre af identitetsoplysninger om juridiske enheder, hvilket eliminerer behovet for, at enheder skal udføre kendskabskrav til deres modparter i finansielle transaktioner og giver dem adgang til pålidelige og aktuelle oplysninger .

Finansielle institutioner i TUPAS-systemet er de eneste enheder, der opbevarer og overfører brugeroplysninger, hvilket giver dem mulighed for at tjene penge på identitet-som-en-tjeneste gennem forretningsmodeller som abonnement eller gebyr-for-transaktion-tjenester med RP'er.

TUPAS

Privat sektorløsning, Finland. I TUPAS-

systemet skal RP'er betale IdP'er (i dette tilfælde et konsortium af banker) for at få adgang til pålidelige og nøjagtige brugerattributter.

Machine Translated by Google

Fremtidige tilstandsapplikationer

Machine Translated by Google

Digital identitet tilbyder FI'er forbedrede og nye muligheder

Ud over de fordele på første niveau ved digital identitet, som finansinstitutter ville modtage som følge af deltagelse i et identitetssystem, har vi undersøgt nogle fremtidsrettede anvendelsesscenarier, der illustrerer yderligere muligheder, som digital identitet kan tilbyde finansinstitutter.

POTENTIELLE FREMTIDIGE ANVENDELSER

1. Skræddersyede risikoprofiler

2. International genbosættelse

3. Attributter knyttet til betalingstokens

4. Digital selvangivelse

5. Fastlæggelse af den samlede risikoeksponering

6. Identifikation af transaktionsmodparter

7. Forbindelse af individuel identitet med virksomhedsidentitet

8. Sporing af samlet genpantsættelse af aktiver

Machine Translated by Google

Hvilke yderligere muligheder kan digital identitet tilbyde FI'er?

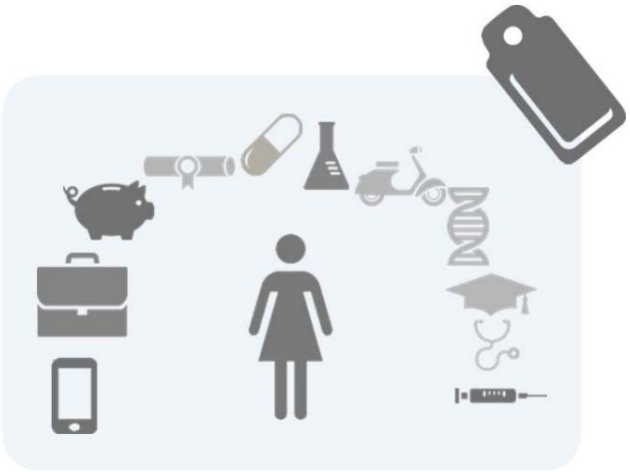
1. SKRÆDDERSYEDE RISIKOPROFILER

NUVÆRENDE TILSTAND:

Finansielle institutioner opretter i øjeblikket risikoprofiler for enkeltpersoner og juridiske enheder ved hjælp af de begrænsede oplysninger, der indsamles, når kunder onboardes, og prædiktive algoritmer til at levere relevante og skræddersyede produkter og tjenester til deres kunder.

HVORDAN VILLE DIGITAL IDENTITET HJÆLPE?

Finansielle institutioner kan med brugerens samtykke udnytte betroede brugerattributter til mere effektivt at opbygge risikoprofiler for deres kunder og dermed skræddersy kredit- og risikobaserede produkter. Denne forbedrede brugeroplevelse vil i sidste ende føre til øget kundetilfredshed og give vækstmuligheder for finansielle institutioner.



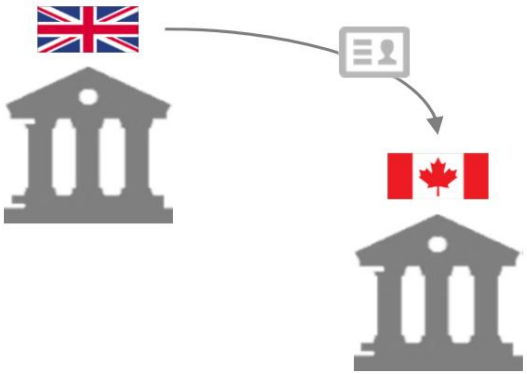
2. INTERNATIONAL GENBOSÆTTELSE

NUVÆRENDE TILSTAND:

Dagens onboarding-processer kræver, at alle FI'er onboarder en kunde fra en nulvidenstilstand, hvilket resulterer i vanskeligheder med at åbne konti for enheder, der ikke kan bevise deres identitet, og tilsidesættelse af finansiel historik.

HVORDAN VILLE DIGITAL IDENTITET HJÆLPE?

Brugere kunne transportere deres digitale identitet på tværs af jurisdiktioner og bruge den til nemt at få adgang til finansielle og andre tjenester i deres nye bopæl. De attesteringer og attributter, der besiddes af brugerens oprindelige FI('er), ville tjene som grundlag for, at nye FI'er kan blive IdP'er. Dette ville eliminere behovet for, at den modtagende FI udfører den dyre og arbejdskrævende "kend din kunde"-proces, der ellers ville være påkrævet. Derudover ville det reducere den tid og indsats, det tager for FI'er at onboarde brugere, og give dem mulighed for at inkorporere pålidelige, historiske oplysninger.



Machine Translated by Google

Hvilke yderligere muligheder kan digital identitet tilbyde FI'er?

3. ATTRIBUTTER KNYTTET TIL BETALINGSTOKENER

NUVÆRENDE TILSTAND:

Når kunderne gennemfører transaktioner, skal de manuelt angive deres attributter (f.eks. bekræftelse af alder, forsendelsesoplysninger) eller bevis for attributter til forhandlerne på salgsstedet.

HVORDAN VILLE DIGITAL IDENTITET HJÆLPE?

Finansielle institutioner kunne automatisk levere kundeattributter til forhandlere, hvilket strømliner og sikrer transaktionsprocessen for både forhandler og kunde. Den digitale overførsel af attributter ville eliminere risikoen for menneskelige fejl i informationsoverførsel og dramatisk reducere informationsafhjælpning og afbrydelse af transaktioner for den registrerede leverandør.

Bemærk: Denne automatiske overførsel af attributter kan understøttes af en yderligere godkendelsesfaktor (f.eks. mobil- eller adfærdsgodkendelse) for at forhindre svindel.

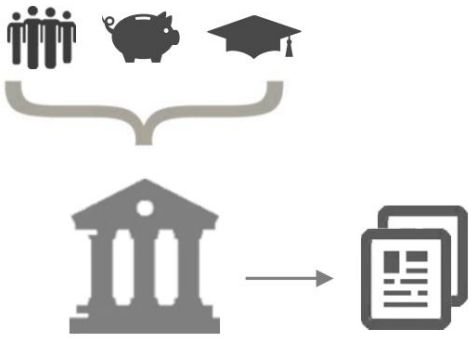
4. DIGITAL SKATTEANMELDING

NUVÆRENDE TILSTAND:

Enkeltpersoner og virksomheder indgiver i øjeblikket deres skatter baseret på aggregering af oplysninger fra flere kilder (f.eks.
Finansinstitutioner, arbejdsgivere, uddannelsesinstitutioner osv.).

HVORDAN VILLE DIGITAL IDENTITET HJÆLPE?

I samarbejde med myndigheder kan skatter udfyldes automatisk og selvangivelser genereres af kundernes valgte finansformidlere ved hjælp af deres fulde viden om kundernes økonomiske beholdninger, aktiver, indkomst og personlige forhold. Med brugerens samtykke vil alle disse oplysninger være tilgængelige via et robust digitalt identitetsnetværk. Dette vil muliggøre en effektiv og præcis skatteindgivelsesproces.



Machine Translated by Google

Hvilke yderligere muligheder kan digital identitet tilbyde FI'er?

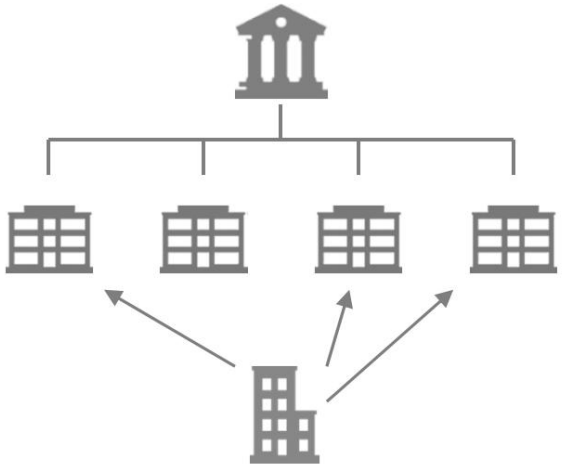
5. FASTSÆTTELSE AF DEN SAMLEDE RISIKOEKSPONERING

NUVÆRENDE TILSTAND:

Juridiske enheder er ofte ikke i stand til at fastslå deres samlede risikoeksponering over for en given modpart på grund af komplicerede ejerstrukturer og vanskeligheder med at få et fuldstændigt overblik over en juridisk enhed.

HVORDAN VILLE DIGITAL IDENTITET HJÆLPE?

Transaktionsmodparter kan have et samlet overblik over virksomhedsstrukturen i de enheder, de handler med, hvilket giver dem mulighed for at bestemme deres samlede risikoeksponering over for den pågældende enhed på tværs af transaktioner og forretningsområder.



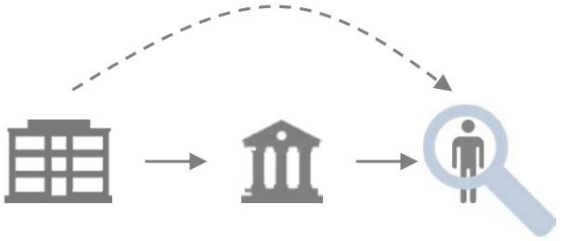
6. IDENTIFIKATION AF TRANSAKTIONSMODPARTIER

NUVÆRENDE TILSTAND:

Det er i øjeblikket udfordrende eller umuligt for enheder at identificere alle enheder, der deltager i en given transaktion; de har muligvis ikke indsigt i slutkunden i en transaktion, der gennemføres af en mægler eller anden modpart.

HVORDAN VILLE DIGITAL IDENTITET HJÆLPE?

Juridiske enheder kan anmode om indsigt i en tredjeparts konsoliderede identitet og ejerskabshistorikken for et givet aktiv involveret i en transaktion. Dette ville give dem mulighed for at identificere både den direkte kunde og slutkunden i transaktionen og dermed bedre informere beslutningen om, hvorvidt transaktionen skal gennemføres.



Machine Translated by Google

Hvilke yderligere muligheder kan digital identitet tilbyde FI'er?

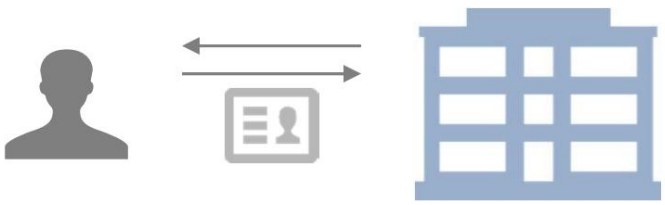
7. FORBINDELSE AF INDIVIDUEL IDENTITET MED VIRKSOMHEDSIDENITET

NUVÆRENDE TILSTAND:

Individuelle og virksomhedsidentitetsoplysninger er i øjeblikket ikke sammenkædet; det er udfordrende at identificere personer, der er tilknyttet virksomheder.

HVORDAN VILLE DIGITAL IDENTITET HJÆLPE?

Digital og standardiseret indsamling, lagring og overførsel af attributter for både enkeltpersoner og juridiske enheder vil sikre, at identitetsoplysninger er nøjagtige og opdaterede. Sammenkoblinger mellem disse systemer vil skabe pålidelige billeder af identiteten på enkeltpersoner tilknyttet juridiske enheder til brug for "kend din kunde" og andre formål.



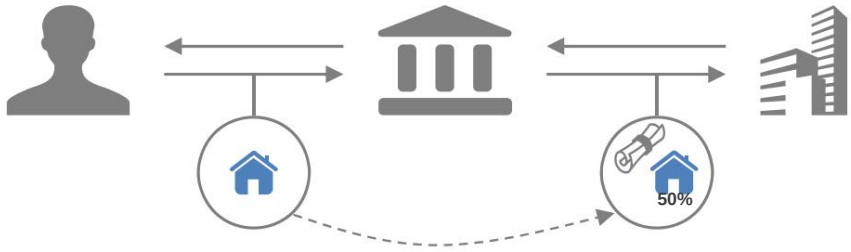
8. SPORING AF SAMLET GENOPRETTELSE AF AKTIVER

NUVÆRENDE TILSTAND:

Transaktions- og ejerskabshistorikken for aktiver kan blive tvetydig, efterhånden som aktiver genpantsættes; dette forværrer modpartsrisikoen og usikkerheden omkring aktivernes værdiansættelse, mens manglen på en historisk sporingsmekanisme forhindrer håndhævelsen af grænser for omfanget af genpantsætning af aktiver.

HVORDAN VILLE DIGITAL IDENTITET HJÆLPE?

Konsoliderede, standardiserede og digitale identitetsoplysninger for aktiver ville være tilgængelige for alle enheder, der deltager i en transaktion, der involverer det pågældende aktiv, hvilket giver transaktionsmodparter mulighed for at kontrollere aktivoplysninger, såsom udsteder og transaktionshistorik. Dette ville muliggøre sporing af aktivernes ejerstruktur og sammensætning og forhindre overhypothekering på grund af manglende indsigt i tidligere transaktioner, der involverer det pågældende aktiv.



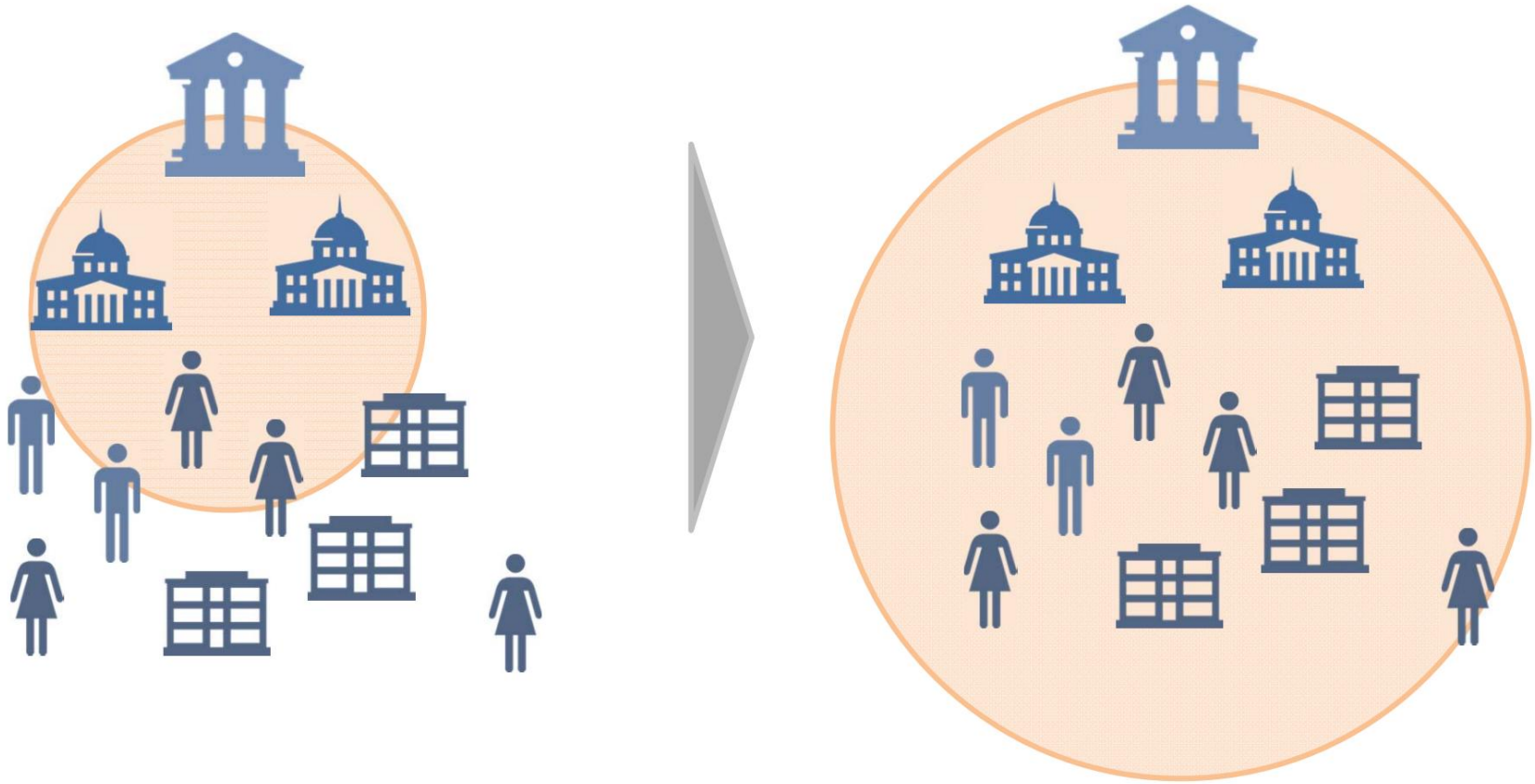
Machine Translated by Google

Implementering af identitet Systemer

Machine Translated by Google

Implementeringen af et digitalt identitetssystem bør følge en bottom-up-tilgang

Vi har skitseret vores perspektiv på de primære drivkræfter inden for digitale identitetsløsninger, og hvordan de bør implementere digitale identitetsløsninger. Det er afgørende at bemærke, at dette er det første skridt i en bottom-up-tilgang, der vil resultere i, at systemer skaleres udad for at inkorporere et større antal brugere, afhængige parter og identitetsudbydere, efterhånden som retningslinjer og funktionalitet testes og forfines.



Systemet lanceres med en kritisk masse af parter til test og forfining

Systemet skaleres til et stigende antal brugere, afhængige parter og identitetsudbydere.

Machine Translated by Google

Global identitet vil aldrig eksistere som en monolit

Dette dokument har fastlagt en principbaseret tilgang til at opbygge effektive, bæredygtige og afgrænsede naturlige identitetsnetværk som fundament for at forbinde individuelle identitetsnetværk. Der vil aldrig være én enkelt, global løsning for identitet.

Identitet tjener forskellige behov

Forskellige brugergrupper har forskellige behov og krav til identitet. Identitetssystemer til enkeltpersoner er designet til at øge brugernes evne til at udføre transaktioner på en sikker måde. Identitetssystemer til juridiske enheder har til formål at muliggøre omfattende aggregering på makroniveau – hvad enten det drejer sig om at bestemme den samlede eksponering for en enkelt juridisk enhed eller at styre systematisk risiko og stabilitet. Identitetssystemer til aktiver er designet til at muliggøre sporing og give gennemsigtighed omkring ejerskab og værdi. Privatliv er et af de vigtigste krav til individuel identitet, men er langt mindre vigtigt i forbindelse med identitet af juridiske enheder og aktiver og kan endda forstyrre de overordnede formål med disse systemer. Enkeltpersoner har selvbestemmelse, hvorimod juridiske enheder og aktiver har depotforvaltere, der handler på deres vegne.

Identitet er kulturel

Identitet påvirkes i høj grad af kulturelle og geopolitiske faktorer. For eksempel, mens nogle befolkningsgrupper er trygge ved at have et nationalt ID-kort, har dette system fejlet i andre jurisdiktioner. Visse myndigheder er muligvis ikke en stabil regering til at fremme skabelsen og indførelsen af digital identitet.

Det betyder, at identitetssystemer, udover at have forskellige konfigurationer af rent praktiske årsager, vil variere dramatisk for at imødekomme de kulturelle og geopolitiske behov, de tjener.

Der findes ingen universel løsning på identitet.

Machine Translated by Google

Et globalt system for identitet kræver derfor i første omgang konstruktionen af diskrete identitetsnetværk og derefter oprettelsen af skinner mellem dem.

At skabe en global løsning for identitet er en proces i to trin: Nøglen til at opbygge et globalt system for digital identitet er først at opbygge succesfulde naturlige identitetsnetværk, der imødekommer de unikke behov og præferencer hos deres brugergruppe og situation, og derefter at opbygge et bindevæv, der skaber interoperabilitet mellem disse systemer.

1

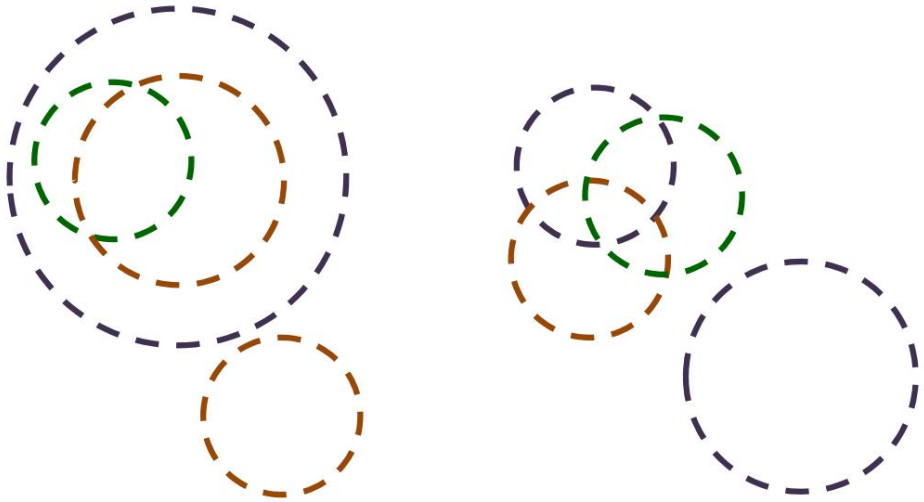
Implementering: Konfiguration af naturlige identitetsnetværk

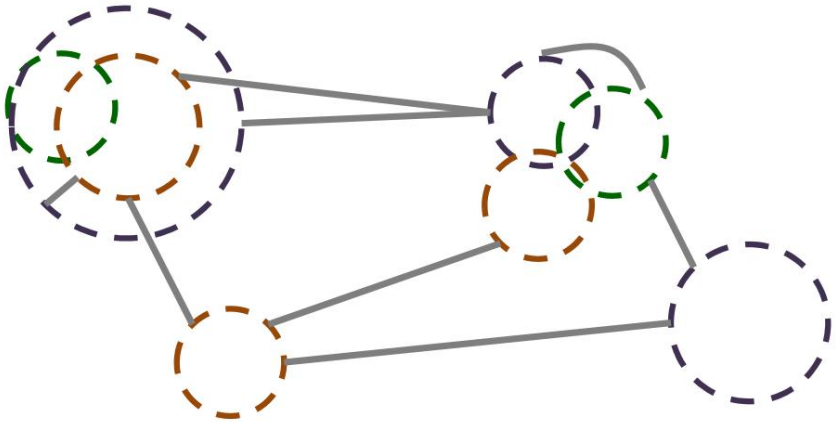
Konfigurationen af naturlige identitetsnetværk vil blive styret af de beslutninger, der træffes i forhold til de primære og sekundære dimensioner af valget

2

Sammenkobling: Bygger skinnerne for global identitet

At bygge skinnerne mellem naturlige identitetssystemer vil skabe global sammenkobling og interoperabilitet



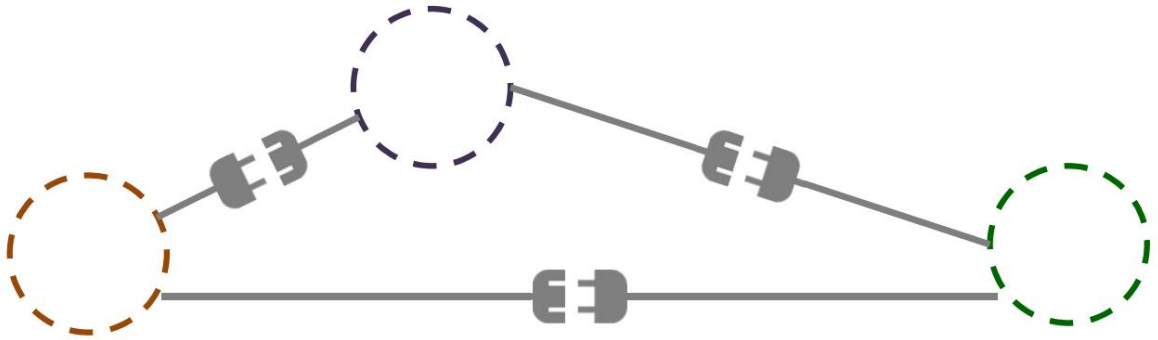


Machine Translated by Google

Selvom skinnerne for global identitet vil begynde at vise sig i takt med at systemerne udvikler sig, er det vigtigt, at enheder følger en vejledende ramme.

Opbygning af identitet som en totrinsproces gør det muligt at bygge identitetssystemer ved at indsnævre de nødvendige interessenter til grupper, der har lignende behov og bekymringer, og derfor har relativt afstemte incitamenter. Det sikrer også, at disse systemer er skræddersyet til de specifikke behov og ønsker hos deres bruger- og interessentgrupper og derfor vil opnå den udbredelse, som et top-down, one-size-fits-all-system ikke ville opnå. Disse løsninger bør dog også bygges efter en fælles ramme, der sikrer interoperabilitet ved at definere funktioner, attributter og krav til de identiteter, der udveksles i systemet. Dette forstærker behovet for, at individuelle identitetssystemer bygges af enheder som f.eks. finansielle institutioner, der har erfaring med at arbejde sammen om at definere standarder, og derefter bygge individuelle systemer inden for disse standarder.

Implementering af separate digitale identitetssystemer, der passer til brugernes unikke behov og kulturelle faktorer i deres egne jurisdiktioner, og design af disse systemer omkring robusthed, interoperabilitet og sammenkobling, vil muliggøre en global skabelon for digital identitet.



Machine Translated by Google

Der er mange stående spørgsmål og usikkerheder, der skal overvejes i forbindelse med oprettelsen af nye identitetssystemer.

NOGLE TANKER TIL AT OPBYGGE IDENTITETSLØSNINGER

Drivere af identitetssystemer bliver nødt til at overveje mange detaljerede taktiske spørgsmål i konfigurationen og implementeringen af deres egne identitetsløsninger. Vi har nedenfor givet nogle eksempler på spørgsmål og usikkerheder.

- Hvilke enheder skal involveres i et identitetssystem for dit område og din brugergruppe – regeringer, regulatorer, finansielle institutioner, forbrugergrupper, andre?

- Hvilken forretningsmodel vil være bæredygtig i den situation – brugeren betaler, den pårørende betaler, staten betaler? Per transaktion, abonnement, subsidieret gennem andre tjenester?

- Hvilken styringsstruktur er nødvendig for systemet – hvem bør involveres, hvad bør omfanget af deres mandat være, hvordan Vil styringen blive fornyet og opdateret?

- Hvad er det minimum levedygtige identitetsprodukt, der kræves i den situation – hvilke brugere skal involveres, hvilke tjenester skal dækket, hvilke enheder bør involveres, hvilke metrikker testes?

- Hvilke rammer og standarder kan anvendes for identitetssystemet?

- Hvilke komponenter i identitetsstakken skal være proprietære, og hvilke kan outsources eller erhverves gennem partnerskab?

- Hvilken teknologiplatform kræves til systemet?

- Hvad er den bedste metode til at kommunikere systemets funktionalitet og fordele til brugerne?

Machine Translated by Google

Kontaktoplysninger

Machine Translated by Google

For yderligere information, kontakt venligst:

VERDENSØKONOMISK FORUMS KERNEPROJEKTTEAM

R. Jesse McWaters

Projektleder, Finansielle Tjenester
Verdensøkonomisk Forum

Jesse.McWaters@weforum.org

Giancarlo Bruno

Seniordirektør, chef for finansielle tjenester
Verdensøkonomisk Forum

Giancarlo.Bruno@weforum.org

PROFESSIONEL SERVICESUPPORT FRA DELOITTE

Christine Robson

Deloitte Canada

crobson@deloitte.ca

Rob Galaski

Deloitte Canada

rgalaski@deloitte.ca

Machine Translated by Google

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD